DATA QUALITY REQUIREMENTS FOR HEALTH CARE IDENTITY MANAGEMENT AND MASTER PERSON INDEX FUNCTIONS

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive establishes the business authority for the VHA Data Quality Health Care Identity Management Program (HC IdM) and defines HC IdM enterprise and business requirements throughout the information systems lifecycle related to: Master Person Index (MPI), other information technology (IT) applications and services that consume person identity, and HC IdM operations at Department of Veterans Affairs (VA) medical facilities.

2. SUMMARY OF MAJOR CHANGES: This VHA directive includes:

a. Updates to authoritative sources for entry of a date of death (see Appendix A, paragraph 2.l.).

b. Updates to organizational entities and notes, including establishing the relationship between the HC IdM and other Departmental entities.

c. Updates to references (see paragraph 8).

d. Responsibilities for VA Governing Bodies such as the VA Data Governance Council and Integrated Project Teams (IPT) (see paragraph 5.h.), Business Owners (see paragraph 5.m.), and Data Stewards (see paragraph 5.r.).

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

3. RELATED ISSUES: VA Directive 6510, VA Identity and Access Management, dated January 15, 2016; VA Handbook 6510 VA Identity and Access Management, dated January 15, 2016; VHA Directive 1907.05, Repair of Catastrophic Edits to Person Identity, dated April 4, 2017; VHA Directive 1604, Data Entry Requirements for Administrative Data, dated April 22, 2016; VHA Directive 1907.09 Identity Authentication for Health Care Services, dated June 6, 2019.

4. RESPONSIBLE OFFICE: The VHA Office of Health Informatics (OHI) (10A7) Data Quality Program is responsible for the contents of this directive. Questions may be addressed at VHAHIGDataQualityProgramLeadership@va.gov.

5. RESCISSIONS: VHA Directive 1906, Data Quality Requirements For Identity Management and Master Veteran Index Functions, dated April 29, 2013, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of April 2025. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

BY DIRECTION OF THE OFFICE OF THE UNDER SECRETARY FOR HEALTH:

/s/ Steven L. Lieberman MD, MBA, FACHE
Acting Principal Deputy Under Secretary for Health

NOTE: *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

DISTRIBUTION: Emailed to the VHA Publication Distribution List on April 13, 2020.

CONTENTS

DATA QUALITY REQUIREMENTS FOR HEALTH CARE IDENTITY MANAGEMENT AND MASTER PERSON INDEX FUNCTIONS

DATA QUALITY REQUIREMENTS FOR HEALTH CARE IDENTITY MANAGEMENT AND MASTER PERSON INDEX FUNCTIONS

1. PURPOSE

This Veterans Health Administration (VHA) directive establishes the business authority for the Health Care Identity Management (HC IdM) Program and defines HC IdM enterprise and business requirements throughout the information systems, as they relate to: Master Person Index (MPI), other information technology (IT) applications and services that consume person identity, and HC IdM operations at Department of Veterans Affairs (VA) medical facilities. MPI is the authoritative identity service within VA maintaining and synchronizing identities for all persons that VA uniquely identifies, e.g., Veterans, beneficiaries, patients, employees, IT users, and health care providers. **AUTHORITY:** Title 38 United States Code (U.S.C.) 7301(b) and 44 U.S.C. 3102.

2. BACKGROUND

a. In Fiscal Year (FY) 2000, VHA established HC IdM, now within the Office of Health Informatics (OHI), Health Information Governance, Data Quality Program, as the national business owner and data steward for MPI and the services and activities needed to maintain and ensure the integrity of a person's longitudinal health record and unique person identity. MPI and the activities performed by HC IdM and the Data Quality Program are based on national standards (i.e., American Society for Testing and Materials (ASTM)). MPI and its services link all records about one person in multiple VHA, VA, Department of Defense (DoD), and other external systems to provide that person's complete electronic health record (EHR). This ability is essential to seamless care coordination, data sharing, and interoperability with health care partners such as DoD and the eHealth Exchange, VA lines of business (LOB), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA).

b. Since 1996 MPI has maintained an entry and unique identifier for all persons who have had an active record in any Veterans Health Information Systems and Technology Architecture (VistA) PATIENT file (#2). Today MPI provides the capability to link a person's records by matching traits such as name, Social Security Number (SSN), date of birth (DOB), birth sex, and address from different data sources. The records are from multiple VA medical facilities' national databases, other VA systems such as MyHealtheVet (MHV), and external sharing partners. Records from VBA systems, employee systems (HR Smart), and other entities within the scope of VA are also included.

c. Current Data Quality Program activities include: establishing business policy and rules; guiding the sharing of identity data with external business partners; guiding specification of and compliance with identity management business requirements as they are implemented in IT applications and services; overseeing core identity management product implementation; and monitoring, identifying, and resolving record identity integrity issues along with conflicts in the MPI, VA systems (such as MHV), and local VA medical facilities. This includes the resolution of duplicate records, mismatches, and overwrites (catastrophic edits) of a person's identity that may affect

patient care and safety. Program activities continue to expand to other VA LOBs which include the implementation, monitoring, identification, and resolution of identity integrity issues and conflicts in the MPI with LOB systems and external sharing partners.

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

e. HC IdM depends on the correct identification of unique individuals, but it is distinct from personnel security and logical access which involve managing persons seeking access to VA resources based on national security standards. In addition to these policies, the VA Security Requirements Steering Committee maintains specific requirements for security and privacy of identity information which can be found at: https://vaww.vha.vaco.portal.va.gov/sites/HDI/SRSC/SRSC%20Requirements/Forms/AllItems.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

3. DEFINITIONS

a. **Affiliates.** Affiliates are individuals who require logical access to VA information systems and/or physical access to VA medical facilities to perform their jobs and who do not fall under the category of Federal employee or contractor. Examples include but are not limited to: Veteran Service Organizations' representatives, The Joint Commission reviewers, child care staff, credit union staff, union officials, and union support staff. See VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, dated October 26, 2015.

b. **Business Owners.** Business Owners are key stakeholders who have the primary business responsibility for governance of a particular software system.

c. **Catastrophic Edit.** Catastrophic edit to person identity means changes have been made to a person's electronic health record in a local EHR system that results in the record being changed inappropriately to that of another person, caused by, but not limited to, edits to person identity data (such as Name, SSN, DOB, Birth Sex) and/or erroneous merging of two or more distinct person records into a single record within the EHR. See VHA Directive 1907.05, Repair of Catastrophic Edits to Person Identity, dated April 4, 2017.

(1) These errors can occur as a result of improper verification by VA staff using the Duplicate Record Merge software application located in VistA when two potential

duplicate person records are not properly reviewed and screened. This results in two different person entries being merged into one.

(2) Errors of this nature can pose a significant patient safety risk at all VA medical facilities.

d. **Data Stewards.** Data Stewards are responsible for the planning, implementing and managing the sourcing, use and maintenance of data assets in an organization.

e. **eHealth Exchange.** VA eHealth Exchange acts as an interface between VA health care systems and the VA eHealth Exchange Gateway so health care information can be successfully exchanged while following applicable security and privacy rules. VA eHealth Exchanges provides a mechanism to make clinical information from multiple sources about Veterans and their dependents available to providers both inside and outside VA in a timely manner.

f. **Electronic Health Record.** EHR is the digital collection of patient health information resulting from clinical patient care, medical testing, and other care-related activities. Authorized VA health care providers may access the EHR to facilitate and document medical care. EHR comprises existing and forthcoming VA software including CPRS, VistA, and Cerner platforms. ***NOTE:*** *The purpose of this definition is to adopt a short, general term (EHR) to use in VHA national policy in place of software-specific terms while VA transitions platforms.*

g. **Health Care Identity Management.** HC IdM comprises a set of business processes and supporting infrastructure for the creation, maintenance, and use of digital identities.

(1) The HC IdM Program is the national business owner and data steward for person identity data within VHA.

(2) The HC IdM Program Staff ensures the integrity of person identity data within the MPI and the associations to the systems that contain EHR information about the person, which provides the longitudinal health record.

h. **Integration Control Number.** Integration Control Number (ICN) is VA's enterprise unique person identifier, based on the ASTM E1714-07 (2013) standard. The ICN is assigned and maintained by the MPI which provides the key to linking records within VA and with external sharing partners.

i. **Master Person Index.** MPI is the authoritative identity service within VA for establishing, maintaining, and synchronizing identities for VA persons, e.g., Veterans, beneficiaries, patients, employees, IT users, and health care providers. MPI contains over 48 million person identities, populated from VA medical facilities, VA Administrations, and external sharing partners (e.g., DoD). MPI facilitates matching and linking of system records entered for a person using a unique identifier, the person's ICN. This enables the sharing of person information and an enterprise-wide view of a person's record including the person's longitudinal EHR.

j. **Primary View.** 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 provides the most authoritative identity traits known about a person's identity within VA.

4. POLICY

It is VHA policy that information systems and databases, including MPI, maintain accurate and complete person-identifying information, and that vital processes related to resolving identity data quality issues be performed. VA medical facility staff must perform vital data quality processes in order to ensure the protection and effective use of person's health information.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive.

b. **Principal Deputy Under Secretary for Health.** The Principal Deputy Under Secretary for Health is responsible for providing oversight for the fulfillment of this directive.

c. **Deputy Under Secretary for Health for Operations and Management.** The Deputy Under Secretary for Health for Operations and Management is responsible for:

(1) Communicating the contents of this directive to each of the Veterans Integrated Services Networks (VISNs).

(2) Ensuring that each VISN Director has sufficient resources to implement this directive in all VA medical facilities within that VISN.

(3) Providing oversight of VISNs to assure compliance with this directive, relevant standards, and applicable regulations.

d. **Assistant Deputy Under Secretary for Health for Health Informatics.** The Assistant Deputy Under Secretary for Health for Health Informatics is responsible for:

(1) Ensuring VHA identity management policies and procedures are comprehensive and implemented throughout VHA.

(2) Providing direction and communication to support VISNs and VA medical facilities with implementation of this directive.

e. **Director, Health Information Governance.** The Director, Health Information Governance is responsible for:

(1) Ensuring the Data Quality and HC IdM Program mission and vision are accomplished by making decisions regarding Data Quality Program resources, funding, and staffing.

(2) Seeking technical guidance on all issues related to identity management from the HC IdM Program Director.

(3) Supporting VHA-wide identity management policies and procedures as written by the HC IdM Program.

f. **Program Director, Data Quality.** The Data Quality Program Director, under the Office of Health Information Governance, is responsible for:

(1) Advising VHA leadership about appropriate use of identity data and services.

(2) Reviewing and updating this directive every 5 years or as needed.

g. **Program Director, Health Care Identity Management.** The HC IdM Program Director is responsible for:

(1) Serving as the VHA business owner and data steward for identity data (e.g., Name, SSN, DOB, Birth Sex, Mother's Maiden Name) maintained within the MPI.

(2) Establishing and maintaining business rules and processes governing person identity management data collection and maintenance.

(3) Ensuring that identity data integrity issues on the MPI, including the resolution of duplicates, mismatches, and catastrophic edits to identity, are continuously monitored and addressed as appropriate.

(4) Identifying and assisting in the improvement of processes and methods to enter person data into EHR systems and the MPI.

(5) Supporting identity matching efforts for data sharing and business partners such as DoD.

(6) Improving the awareness and understanding of the MPI, including its roles and functions, across VA, DoD, other related government agencies, and external groups.

(7) Providing information and training to users at all levels of the organization. See paragraph 6.

h. **Chairperson, VA Governing Bodies.** The chairperson of the governing bodies within VA, such as the VA Data Governance Council and Integrated Project Teams (IPT) has agreed to be responsible for:

(1) Making decisions regarding business requirements, service requests and management, acquisition efforts, documentation efforts, risks, and issues. Issues are brought to the governing bodies based upon their group scope of responsibility and expertise.

(2) Serving as advocates for common standards and specifications for a secure, trusted, interoperable person-centric record, by making recommendations and

publishing guidance.

i. **Veterans Integrated Service Network Director.** The VISN Director is responsible for:

(1) Ensuring that the entry of person identity data into VHA applications is accurate, complete, and associated only with the person to whom the data belongs in each VA medical facility within their control.

(2) Ensuring VHA identity management policies and procedures are implemented within each VA medical facility.

j. **VA Medical Facility Director.** Each VA medical facility Director is responsible for:

(1) Ensuring that the entry of person identity data into VHA applications by VA medical facility staff is accurate and complete.

(2) Ensuring that local duplicate person records are reviewed and merged by the VA medical facility MPI Point of Contact (POC) or other qualified staff, in VA EHRs using the appropriate identity maintenance software. This process must be done in an accurate manner as soon as possible after identification and verification that the records belong to the same person.

(3) Designating individuals as MPI POCs who are responsible for resolving identity issues on a daily basis, as well as merging local duplicate person records and resolving any other identity data quality issues brought to their attention.

(4) Ensuring that personnel are assigned to resolve, in an appropriate timeframe, issues with communication links, infrastructure, and applications that support data communications. This includes assigning VA staff members to the following roles (including alternates for each role):

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

(b) Office of Information and Technology (OIT) IT Operations and Services (ITOPS) MPI POC.

(5) Ensuring that administrative service chiefs, supervisors, and staff are made aware of policies and procedures related to catastrophic edits to person identity. This includes ensuring all staff with the ability to enter, edit, and/or merge person identity data (such as Name, SSN, DOB, and Birth Sex) are required to complete and document the required training module "Prevention of Catastrophic Edits to Person Identity."
NOTE: *The required training "Prevention of Catastrophic Edits to Person Identity," can be found at VA Learning University Talent Management System (TMS) under Item Number VA 7861 at www.tms.va.gov. This is an internal VA Web site that is not available to the public.*

(6) Ensuring that the supervisors of staff who can create or edit identity records are responsible for managing the successful completion and documentation of "Prevention of Catastrophic Edits to Person Identity" training by employees, as this is a key competency for identity management (see paragraph 6). Any individual who does not demonstrate competency of patient selection and correctly editing identity traits must re-take the training until core competency is established. Any individual who incorrectly selects, edits, or merges a person's record and generates a catastrophic edit or merge to a person's record must re-take the training and provide evidence of successful completion to the individual's supervisor and the HC IdM Program Staff.

(7) Ensuring supervisors monitor employee work quality and ensure employees achieve and maintain core competency of patient selection and correctly editing identity traits; failure to achieve competency can lead to patient safety issues.

(8) Designating an Administrative MPI POC to identify potential catastrophic edits and notify the HC IdM Program staff. If a verified catastrophic edit is found, the MPI POC must work with the HC IdM Program staff to restore the records involved. The MPI POC will perform daily maintenance activities, including reviewing catastrophic edit alerts, bulletins, and other related tasks. See VHA Directive 1907.05 for detailed procedures and timelines in correcting health and identity information within the EHR and other electronic databases when identity data are erroneously associated with a different person as a result of a catastrophic edit to person identity.

(9) Ensuring that all VA medical facility staff involved in editing or altering the EHR exercise care and caution when making changes to identity traits of persons and report any suspected catastrophic edits to the designated VA medical facility Administrative MPI POC.

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

(11) Ensuring that each supervisor involved in the activities of entering demographic data follows the guidance on data quality of the administrative and demographic elements provided by the VHA Office of Community Care. See VHA Directive 1604, Data Entry Requirements for Administrative Data, dated April 22, 2016.

(12) Ensuring that staff members responsible for data entry of administrative and demographic information are informed of the requirements mandated by the VHA Office of Community Care.

(13) Ensuring that the audit trail for identity traits in all EHRs is maintained and never purged as this is critical in the identification and resolution of catastrophic edits to person identity and other identity integrity issues.

(14) Ensuring all suspected cases of medical identity theft are investigated by VA medical facility staff and if verified to be theft, reported to the appropriate Regional Counsel and Office of Inspector General (OIG). Edits to the person record must not be made until after the OIG investigation has been completed. ***NOTE:*** *Specific information regarding these processes can be found in Appendix A, paragraph 4.*

k. **VA Medical Facility Chief of Health Information Management.** The VA medical facility Chief of Health Information Management (HIM), or equivalent, is responsible for ensuring the VA medical facility staff under their direction review potential duplicate records. This is to verify whether or not the records should be merged (see Appendix A, paragraph 5).

l. **VA Medical Facility Supervisors.** The supervisors of the staff who create, edit, and/or merge patient identity records are responsible for:

(1) Ensuring training requirements are successfully completed and documented by the employee including the "Prevention of Catastrophic Edits to Person Identity" training prior to being given the ability to enter, edit, and/or merge person identity data. See paragraph 6 for additional training information.

(2) Monitoring work quality of staff and ensuring they achieve and maintain core competency of data quality skills. The failure to achieve competency can lead to patient safety issues.

(3) Following the guidance on data quality of the demographic data provided by the VHA Office of Community Care, if the supervisor is involved in the activities of entering demographic data. See VHA Directive 1604.

(4) Ensuring that each staff member involved in the activities of entering demographic data follows the guidance on data quality of the administrative and demographic or non-identity elements provided by the VHA Office of Community Care. See VHA Directive 1604.

m. **VA Medical Facility Administrative Master Person Index Point of Contact.** Each VA medical facility Administrative MPI POC is considered to be the liaison between the VA medical facility and HC IdM. MPI POCs are responsible for:

(1) Working with MPI POCs at other VA medical facilities and national HC IdM Program staff in correcting anomalies and addressing issues related to identity data for shared persons.

(2) Taking appropriate action to resolve data quality and other identity issues in the EHR.

(3) Responding to requests from national HC IdM Program staff to resolve catastrophic edits that overwrite the original person entry with another person. Requests must be acknowledged within 1 business day.

(4) Resolving any other identity data quality issues brought to their attention by the national HC IdM Program staff.

(5) Using the Identity Management Toolkit Point of Contact Request system function to facilitate communications.

(6) Ensuring encryption security certificates are available to be utilized when transmitting and receiving person identifiable information.

(7) Obtaining the necessary EHR access to verify identity information.

(8) Making appropriate changes to person data in the respective VA medical facility's EHR system and perform POC functions, such as resolving identity data quality issues.

(9) Ensuring that national HC IdM Program staff are apprised of changes to local POCs by updating contact information in the Identity Management Toolkit "Point of Contact Management" feature.

(10) Providing the appropriate official supporting documentation for requests to change identity data to the HC IdM Program Staff for processing via the Identity Management Toolkit (see Appendix A, paragraph 1.c.).

n. **VA Medical Facility Office of Information Technology Point of Contacts.** VA medical facility OIT POCs are responsible for:

(1) Working with their counterparts and VA OIT Product Development (PD) Product Support 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 identity traits for all EHRs is maintained and never purged as this is critical in the identification and resolution of catastrophic edits to person identity and other identity integrity issues.

(3) Facilitating the resolution of any catastrophic edits to person identity, which must be completed within the timelines designated in VHA Directive 1907.05.

o. **VA Medical Facility Privacy Officer.** The VA medical facility Privacy Officer is responsible for reviewing all documentation supplied by an individual requesting changes (or "amendment requests") to identity data, other than administrative corrections (i.e., typos and misspellings) to ensure it meets the appropriate criteria. If the criteria is met, they are responsible for approving the change and transmitting this information to the MPI POC (see Appendix A, paragraph 1.c.).

p. **National Health Care Identity Management Program Staff.** HC IdM Program staff are responsible for:

(1) Ensuring the integrity of person identity data within MPI and the associated systems that contain identity information about the person.

(2) Conducting a comprehensive review of any potential catastrophic edits to person identity. In the event a catastrophic edit has occurred, they are responsible for notifying the VA medical facility MPI POC of a catastrophic edit at their facility and monitoring the restoration of the person records until complete. The HC IdM Program staff members will make the initial determination as to which person's record is to be restored and which person will have a new record created. If needed, the MPI POC will be asked to assist in the decision making. See VHA Directive 1907.05.

(3) Reviewing and updating as needed the "Preventing Catastrophic Edits to Person Identity" training in TMS (see paragraph 6).

(4) Maintaining current VA medical facility MPI POC contact information in the Identity Management Toolkit.

(5) Working with OIT development and support staff to:

(a) Develop business rules and software requirements related to identity management, perform usability tests, and review draft user manuals of updates to the MPI and the Identity Management Toolkit application;

(b) Identify and report issues with the operation of the MPI and function of the Identity Management Toolkit application; and

(c) Submit service tickets through the trouble ticketing system when assistance is needed from support teams.

(6) Providing training and guidance to MPI POCs about the MPI and use of the Identity Management Toolkit.

(7) Providing guidance and expertise on identity management and the MPI to VA identity management stakeholders including national VA programs and other Federal agencies.

q. **Business Owners.** Business Owners can be affiliated with local VA medical facilities or at the national program level depending upon the context. Business Owners are responsible for:

(1) The functionality and requirements provided by the systems of their business area.

(2) Collaborating with OIT development and Data Quality Program staff to help ensure implementation of identity management requirements.

r. **Data Stewards.** Data Stewards are responsible for:

(1) Planning, implementing and managing the sourcing, use and maintenance of data assets.

(2) Collaborating with the Data Quality Program staff to provide support, guidance,

and input into the development of any policies, guidance, business requirements, and other activities to support identity management.

6. TRAINING

a. The following training is required for all VA staff who will be able to enter, edit, and/or merge person identity data: "Prevention of Catastrophic Edits to Person Identity," which can be found in TMS under Item Number VA 7861, https://logon.iam.va.gov/affwebservices/public/saml2sso?SPID=https://www.successfactors.com/VAHCM03. This training is a key competency for identity management. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

b. Any individual who does not demonstrate competency of patient selection and correctly editing identity traits must re-take the "Prevention of Catastrophic Edits to Person Identity" training until core competency is established. Any individual who incorrectly selects, edits, or merges a person's record and generates a catastrophic edit or merge to a person record must take the refresher training course and provide evidence of successful completion to the individual's supervisor and the HC IdM Program Staff. "Preventing Catastrophic Edits to Patient Identity – Refresher" training can be found in TMS under Item Number 29287.

7. RECORDS MANAGEMENT

All records regardless of format (e.g., paper, electronic, electronic systems) created in this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VA Records Control Schedule 10-1. Questions regarding any aspect of records management should be addressed to the appropriate Records Manager or Records Liaison.

8. REFERENCES

a. 44 U.S.C. 3102.

b. 44 U.S.C. 3501, et seq.

c. 38 U.S.C. 7301(b).

d. VA Directive 6507, Reducing the Use of Social Security Numbers, dated November 20, 2008.

e. VA Directive 6510, VA Identity and Access Management, dated January 15, 2016.

f. VA Handbook 6510, VA Identity and Access Management, dated January 15, 2016.

g. VHA Directive 1341(1), Providing Health Care for Transgender and Intersex Veterans, dated May 23, 2018.

h. VHA Directive 1601A.02, Eligibility Determination, dated November 21, 2018.

i. VHA Directive 1604, Data Entry Requirements for Administrative Data, dated April 22, 2016.

j. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

k. VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019

l. VHA Directive 1907.05, Repair of Catastrophic Edits to Person Identity, dated April 4, 2017.

m. VHA Directive 1907.09, Identity Authentication for Health Care Services, dated June 6, 2019.

n. VHA Handbook 1601A.01, Intake Registration, dated November 5, 2009.

o. Identity Management Business Requirements Guidance, Version 2.6a, May 2013: https://vaww.vha.vaco.portal.va.gov/sites/HDI/DQ/Business%20Product%20Management/Identity%20Management%20Requirements%20Guidance/Identity%20Management%20Business%20Requirements%20Guidance%20v2_6a.pdf. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

p. The VHA Identity Management Fact Sheet – Identity Trait Changes and VA Identify Management Policy Memorandum (VAIQ 7011145) can be found under the Directives & Guidelines section of the HC IdM Program website at: http://vaww.vhadataportal.med.va.gov/PolicyAdmin/HealthcareIdentityManagement.aspx. ***NOTE:*** *This is an internal VA Web site that is not available to the public*.

q. ASTM E1714-07 (2013). Standard Guide for the Properties of a Universal Healthcare Identifier. (UHIC); Committee E31 on Healthcare Informatics reference: http://www.astm.org.

r. Object Management Group (OMG) Person Identification Service (PIDS) Specification Version 1.1: http://www.omg.org/spec/PIDS/.

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

1. DATA ENTRY AND MAINTENANCE PROCEDURES

a. It is imperative that Department of Veterans Affairs (VA) staff take the utmost care when entering identity data for persons. The leading cause of duplicate entries in the Master Person Index (MPI) and the failure to link records via the Integration Control Number (ICN) is inaccurate or incomplete data (including typographical errors). The following guidelines are intended to increase the accuracy and completeness of essential identity data traits by emphasizing the intended use within Veterans Health Information Systems and Technology Architecture (VistA), clarifying practices to be followed when data is not available or duplicate entries exist, and following established standards, policies, and best practices. Each and every time VA staff are in contact with persons, it is important that identity data for that person be reviewed for accuracy, completeness, and updated, as necessary.

b. The SOCIAL SECURITY NUMBER (SSN), DATE OF BIRTH (DOB), MOTHER'S MAIDEN NAME (MMN), PLACE OF BIRTH [POB CITY], PLACE OF BIRTH [POB STATE], and PLACE OF BIRTH [POB COUNTRY] identity trait fields are important and are to be collected for the unique identification of persons, since these fields generally do not change over time. If these fields are inaccurate or incomplete, it is difficult to ensure duplicate records are not being created. It is also difficult to ensure records are linked to the correct ICN on the MPI. ***NOTE:*** *Collection and use of SSNs must be in compliance with VA Directive 6507, Reducing the Use of Social Security Numbers, dated November 20, 2008, because of a compelling business need under the mission of VA.*

c. Requests to change static administrative data, other than administrative corrections (i.e., typos and misspellings), are considered Privacy Act amendment requests and must be made in writing by the individual or by a personal representative as defined in Veterans Health Administration (VHA) Directive 1605.01, Privacy and Release of Information, dated August 31, 2016. The VA medical facility Privacy Officer must review all documentation supplied by the person to ensure it meets the appropriate criteria and transmit this information to the MPI Point of Contact (POC). The MPI POC is responsible for providing the appropriate official supporting documentation to the Health Care Identity Management (HC IdM) Program Staff for processing via the Identity Management Toolkit.

2. GUIDANCE ON IDENTITY DATA ELEMENTS

a. **NAME.** The NAME field is an important element in the unique identity of a person. Therefore, it is required that the individual's full and complete legal name, including a full middle name, when applicable, be entered. Nicknames or ambiguous information must not be used. Additional guidance for the entry of the name field includes the following procedures:

(1) All data must be entered using uppercase letters.

(2) Commas, apostrophes, and hyphens are the only punctuation permitted in the name.

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

(4) When entering a full name, it must contain a comma (e.g., LASTNAME,FIRSTNAME). Individuals with a legal name as a single value can only be entered as a last name, followed by a comma, as this is a required field.

(5) Multiple last name components must be separated by spaces or hyphens as applicable.

(6) Legal Spanish names are entered in the Last Name field with the father's last name first, a hyphen (or space), and then the mother's maiden name.

(7) Enter full middle names when applicable. A middle initial, without punctuation, is only used if it is the person's given middle name. If a middle name does not exist, this field will remain blank; NMI (no middle initial) or NMN (no middle name) must not be used.

(8) Multiple first (given) names and/or middle names should be entered using the entire name.

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

(10) If entering a Prefix, (such as MR, MRS, MS, and MISS), punctuation must not be used.

(11) 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.

(12) If the person has had a legal name change, a record amendment request must be submitted in writing, by the person, along with official supporting documentation to the VA medical facility MPI POC.

(13) Marriage licenses, or certificates, or divorce decrees are not sufficient stand-alone documents for a name change, as not all people who apply for a marriage license, or marry, or get divorced change their name. ***NOTE:*** *Refer to the "Identity Management Fact Sheet – Identity Trait Changes" for (1) appropriate official supporting documentation needed for correction to a name component and (2) appropriate supporting legal documentation for a name change. Complete removal of any name*

component or changing any full name component to an initial requires an official name change court order. The Identity Management Fact Sheet – Identity Trait Changes can be located at: http://vaww.vhadataportal.med.va.gov/Portals/0/DataQualityProgram/HCIdM/IdM_Fact_Sheet_Identity_Trait_Changes.docx?web=1. This is an internal VA Web site that is not available to the public.

b. **PREFERRED NAME.** Enter the person's preferred name by which they wish to be addressed in the Preferred Name field in VistA. This name should be used to refer to the person during any clinical or administrative interactions at a VA medical facility. The preferred name is not required to be the same as their legal name. The identity field Preferred Name was created to retain and manage the name by which the person wished to be identified. The Preferred Name is part of the person's demographic information and is not used in identity record matching.

c. **SOCIAL SECURITY NUMBER.**

(1) Enter the person's current official SSN issued by the Social Security Administration. No other value will be entered into this field. If a valid SSN is not known or the person refuses to provide an SSN, then a "P" must be entered into the field for the calculation of a pseudo SSN. SSNs must not 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 persons and are not to be used for any other purpose.

(2) An amendment request to change the SSN requires that the individual submit the request in writing, along with supporting documentation that displays the different SSN, to the MPI POC at a VA medical facility. However, in the case of administrative corrections, there are instances where the SSN can be verified and corrected without requiring documentation from the individual. ***NOTE:*** *Refer to the "Identity Management Fact Sheet – Identity Trait Changes" for a list of supporting documentation sources at: http://vaww.vhadataportal.med.va.gov/Portals/0/DataQualityProgram/HCIdM/IdM_Fact_Sheet_Identity_Trait_Changes.docx?web=1. This is an internal VA Web site that is not available to the public.*

d. **BIRTH SEX AND SELF IDENTIFIED GENDER IDENTITY.**

(1) Male or Female must be entered in the BIRTH SEX field as consistent with the person's original birth certificate. This allows for automatic clinical reminders, lab results, medication dosages, etc. to provide correct values within the EHR and ensure optimal care for the person. If a person's birth sex was entered in error it can be corrected as a remedial action by administrative personnel with the authority to correct information previously entered in error.

(2) In order to alleviate the need for changing the Birth Sex from its original value on person records, the self-identified gender identity (SIGI) field has been added to VistA and the MPI. This field is intended to signify the person's gender preference so VA staff

can determine the appropriate way to communicate with them. This field is available for updating in VistA and will display within MPI and other VA applications in time. The SIGI field may be set as desired by the person and requires no documentation for updates.

(3) Some persons will want to change their Birth Sex entry to reflect their identity and this is the person's right. Surgery is not a prerequisite for amendment of Birth Sex. A person's request for amendment to Birth Sex in their record is considered a Privacy Act "amendment request". ***NOTE:*** *Refer to the "Identity Management Fact Sheet – Identity Trait Changes" for a list of documentation required for editing the BIRTH SEX field at: http://vaww.vhadataportal.med.va.gov/Portals/0/DataQualityProgram/HCIdM/IdM_Fact_Sheet_Identity_Trait_Changes.docx?web=1. This is an internal VA Web site that is not available to the public.*

e. **DATE OF BIRTH.**

(1) 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 date of birth (DOB) is not available. If DOB is unknown 01/01/1900 must be entered.

(2) Correction of errors in the DOB field does not require processing by the HC IdM Program Staff. The VA medical facility must correct the DOB after obtaining the proper verification of the correct DOB. *Refer to the "Identity Management Fact Sheet – Identity Trait Changes" for a list of supporting verification sources at: http://vaww.vhadataportal.med.va.gov/Portals/0/DataQualityProgram/HCIdM/IdM_Fact_Sheet_Identity_Trait_Changes.docx?web=1. This is an internal VA Web site that is not available to the public.*

f. **MOTHER'S MAIDEN NAME.** Enter the last name only of the individual's mother at the time of her birth. This field will remain blank if unknown or not provided; "DECEASED," "UNKNOWN," and other inappropriate responses must not be used.

g. **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.

h. **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.

i. **PLACE OF BIRTH [COUNTRY] (NOT YET AVAILABLE).** Enter the birth country only (future implementation in VistA). The default country is the UNITED STATES.

j. **MULTIPLE BIRTH INDICATOR.** Enter YES in the MULTIPLE BIRTH INDICATOR (MBI) field only if the person is part of a multiple birth (e.g., is a twin, triplet). This field assists in the unique identification of individuals who are part of a multiple birth and may have identity traits similar to other person entries. The field must be left blank if it is unknown or not provided.

k. **ALIAS FIELDS.** The ALIAS fields must only be used to enter previously-used names and SSNs. Former names due to legal name changes (e.g., marriage, divorce, gender change), are to be entered into the ALIAS field. An entry in this field is automatically cross-referenced and the record can be located using the alias name.

l. **DATE OF DEATH.** Death certificates are generally required to enter a Date of Death. Date 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. VA medical facilities are required to use the following as authoritative sources in order of precedence.

(1) The VA medical facility if the person died in the VA medical facility or while under VA auspices,

(2) Death Certificate,

(3) Electronic Verification of Vital Events (EVVE) death certification,

(4) EVVE Fact of Death query results that provide minimum matching traits specified by HC IdM,

(5) NCA if the Veteran has received burial benefits, or

(6) Documentation of death received while establishing death in accordance with 38 CFR 3.211 and 3.212.

m. **MOTHER'S NAME AND FATHER'S NAME.** The person's mother's and father's complete legal names must be entered in the appropriate fields, when known; "deceased," "unknown," and other inappropriate responses must not be used.

3. NONTYPICAL PERSONS

a. **Incapacitated, Unidentified, or Unresponsive Persons (for Whatever Reason).** In VistA, records for incapacitated, unidentified, or unresponsive persons must be entered with a pseudo SSN, 01/01/1900 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. Records must be completed with appropriate identity data trait fields once the patient has been identified. In the joint VA-DoD system the nomenclature for incapacitated, unidentified, or unresponsive persons will be determined as the implementation is finalized.

b. **TEST Persons.** It is essential that TEST persons who exist in production systems be designated with an SSN containing five leading zeros (i.e., 000001111) and the last name prefixed by ZZ (i.e., ZZTESTPATIENT, FIRSTNAME MIDDLE). Test entries are 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 Health Care Identity Management (HC IdM) Program Manager.

c. **Research Patients.** Research patients must have all valid information (e.g., legal name, real SSN, DOB) collected and entered.

4. MEDICAL IDENTITY THEFT

a. **Patient Records Involved in Medical Identity Theft.** In the event that the identity of an existing person is stolen, the information belonging to the identity thief must be retracted from the existing record and attributed to the correct individual by the designated VA medical facility staff listed in paragraph 4.b. of this appendix. If the identity thief cannot be identified, the record shall be established with the NAME field of THEFT,IDENTITY A, where the trailing letter would be incremented for each subsequent entry that exists in the local EHR (e.g., THEFT,IDENTITY B then THEFT,IDENTITY C). The record must be edited to use a pseudo SSN and have the DOB recorded as 01/01/1900.

b. **Reporting of Medical Identity Theft.** Any VA medical 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 Office of Community Care Manager or equivalent. These individuals are responsible for notifying the Administrative MPI POC, HC IdM Program Staff, VA medical facility management staff, VA medical facility Police Service, VA medical facility Information Security Office, VA medical facility Privacy Officer, VA medical facility Compliance Officer, appropriate Regional Counsel, and the Office of Inspector General (OIG). Edits to the person record must not be made until after the OIG investigation has been completed. Any electronic documentation that is determined not to belong to the real person (if identified) must be retracted in the same manner that any document found to be erroneously attributed to a person is removed.

5. DUPLICATE PERSON ENTRIES

a. Merging of local duplicate person records must be performed in an accurate manner and the merge process initiated within an appropriate timeframe after identification by the MPI POC. When more than one record exists for the same person a treating clinician may not see a complete view of the care provided to a person and may make treatment decisions based on a fragmented record.

b. 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. It is essential that appropriate VA medical facility staff review potential duplicate records, to verify whether or not they should be merged.

6. CATASTROPHIC EDIT TO PERSON IDENTITY

A catastrophic edit to person identity occurs when changes are made to a person's EHR that results in the record being changed inappropriately to that of another person. A catastrophic edit can be caused by, but not limited to, edits to person identity data

(Name, SSN, DOB, and Birth Sex) and/or erroneous merging of two or more distinct person records into a single record within the EHR. Refer to VHA Directive 1907.05, Repair of Catastrophic Edits to Person Identity, dated April 4, 2017 for detailed procedures and timelines in correcting health and identity information within the EHR and other electronic databases when identity data are erroneously associated with a different person as a result of a catastrophic edit to person identity.