

December 19, 2012

VHA SOCIAL SECURITY NUMBER REDUCTION

1. PURPOSE: This Veterans Health Administration (VHA) Directive establishes policy for all VHA facilities and Program Offices regarding the reduction and elimination of all unnecessary use of Social Security Numbers (SSN) as the primary identifier for Veterans and employees within VHA; this includes VHA data managed, or retained in, contractor-owned, managed, or operated systems, and applies to all existing or new uses of the SSN. **AUTHORITY: Office of Management and Budget (OMB) Memorandum 07-16.**

2. BACKGROUND

a. The Office of Management and Budget (OMB) issued Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, on May 22, 2007. In this memorandum, OMB mandated that Federal agencies review their use of SSNs in agency systems and programs to identify where the collection or use of a SSN is unnecessary. The memorandum gave agencies 120 days from May 22, 2007 to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. Since 2008, OMB has required each Federal agency to update and submit its SSN reduction and elimination plan as part of the annual Federal Information Security Management Act (FISMA) report.

b. Use of the SSN includes the SSN in any form, including, but not limited to: truncated, masked, partially masked, scrambled, encrypted, or otherwise disguised. Security protections are in place to protect SSNs that are authorized and approved for new or continued collection and use within VHA.

c. The Department of Veterans Affairs (VA) is researching alternative identifiers to the SSN. SSNs will continue to be collected and used as necessary for identification purposes until a solution is in place. **NOTE:** *See Attachment A, Social Security Number Alternatives.*

3. POLICY: It is VHA policy that the use of the SSN must be limited to only those transactions that specifically require, or are authorized for, the presentation of the SSN to meet a statutory requirement, regulatory requirement, or compelling business need.

NOTE: *For examples of acceptable uses of the Social Security Number, see VA Handbook 6507.1, Acceptable Uses of the Social Security Number (SSN) and the VA SSN Review Board.*

4. ACTION

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for:

(1) Establishing and monitoring a SSN Reduction Plan for VHA.

THIS VHA DIRECTIVE EXPIRES DECEMBER 31, 2017

VHA DIRECTIVE 2012-035

December 19, 2012

(2) Ensuring VHA Chief Officers, Veterans Integrated Service Network (VISN), facility Directors, and Program Offices fulfill their responsibilities related to VHA's SSN Reduction Plan.

b. **VHA SSN Review Board.** The VHA SSN Review Board is responsible for:

(1) Reviewing the current VHA SSN uses from the VA SSN inventory database and proposed use justifications.

(2) Preparing recommendations for the VA SSN Review Board's approval for the new or continued SSN collection and use.

c. **VHA Privacy Office.** The VHA Privacy Office is responsible for:

(1) Keeping a current roster of individuals responsible for SSN reduction plan locally, e.g., Privacy Officers at VA medical facilities.

(2) Maintaining the VHA SSN inventory database documenting all approved uses of the SSN within VHA.

(3) Participating regularly in the VA SSN Working Group.

(4) Providing annual refresher training to Privacy Officers on collection and use of the SSN.

(5) Providing bi-annual input to the VA Privacy Service on the progress of VHA's reduction and elimination activities for inclusion in the Federal Information Security Management Act (FISMA) annual report.

(6) Submitting bi-annual report to VA Privacy Service, which include regular updates to VHA's SSN reduction plan and changes in the implementation plan for the OMB submission.

d. **VHA Chief of Staff, or designee.** The VHA Chief of Staff or designee is responsible for ensuring that all new VHA forms that require a SSN have been approved by the VHA SSN Review Board. *NOTE: These forms will need to have final approval by the VA SSN Review Board.*

e. **VISN Directors, VHA Facility Directors and VHA Program Officers.** VISN Directors, VHA Facility Directors and VHA Program Officers are responsible for:

(1) Reviewing or delegating responsibility for review of all information collections that currently use SSNs as an identifier.

(2) Adhering to VA Handbook 6507.1, Acceptable Uses of the Social Security Number (SSN) and the VA SSN Review Board, to determine acceptable use criteria.

(3) Evaluating, on a facility level, alternative mechanisms and processes to using the SSN.

(4) Collaborating with the VHA Privacy Office to determine acceptable usage of the SSN on a facility level and providing justification of continued usage to the VHA SSN Review Board when necessary.

(5) Implementing appropriate controls to improve security and protect the privacy of SSNs where continued collections and uses have been approved.

f. **Facility Privacy Officers and VHA Program Offices.** VHA Facility Privacy Officers and VHA Program Offices are responsible for:

(1) Serving as a primary point of contact for the VHA SSN Reduction and Elimination initiative.

(2) Evaluating on a facility or Program Office level any unnecessary uses of the SSN, eliminating or minimizing the SSN to meet the facility or Program Office business need.

(3) Ensuring updates are made to the VA SSN inventory database (e.g., plans of action and milestones and remediation).

(4) Attending ad hoc conference calls and meetings as directed by the VHA Privacy Office.

(5) Submitting quarterly report updates (according to established deadlines) on SSN reduction and elimination efforts to the VHA SSN Review Board.

5. REFERENCES

a. The President's Task Force on Combating Identity Theft: Strategic Plan, April 2007.

b. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.

c. VA Directive 6507, Reducing the Use of Social Security Numbers.

d. VA Handbook 6507.1, Acceptable Uses of the SSN and the VA SSN Review Board.

e. VHA Directive 1605, VHA Privacy Program.

f. VA Handbook 6500, Information Security Program.

6. FOLLOW-UP RESPONSIBILITY: The Director, Information Access & Privacy (10P2C1), Health Information Governance, VHA Office of Informatics and Analytics, is responsible for the contents of this VHA Directive. Questions may be addressed at 704-245-2492.

7. RESCISSION: NONE. This VHA Directive expires December 31, 2017.

VHA DIRECTIVE 2012-035
December 19, 2012

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

Attachment

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 12/28/2012

December 19, 2012

ATTACHMENT A

SOCIAL SECURITY NUMBER ALTERNATIVES

A primary reason many systems, processes, and forms shifted to use of the Social Security Number (SSN), is that it provides a greater efficiency and requires individuals to remember a single identifier. To counteract the vulnerability that this expanded use of the SSN created, alternatives to the SSN must be used whenever possible. Alternatives include:

a. **Department of Veterans Affairs (VA) Unique Identifier.** VA is exploring options to implement one or more unique identifiers for all Veterans such as the Integration Control Number (ICN) and the Electronic Data Interchange Personal Identifier (EDIPI). VA must provide the specific timeline for implementation and policy for use of these alternatives once determined. SSNs will continue to be collected and used as necessary for identification purposes until a solution is in place.

b. **Net-Centric Environment.** A net-centric environment is a growing number of systems and processes that rely on authentication of individuals with a minimum of collection and storage of SSNs. These systems and processes rely on an authoritative data source as the storage of these SSNs, and access to that information is granted on an “as needed” basis.

c. **Elimination of Identifier.** Many instances where the SSN is collected or used may be able to be eliminated. The technology associated with newer applications is such that it is possible to identify an individual through other pieces of information, negating the need for a unique identifier. This is particularly true of applications that are finite in scope and do not interoperate with other applications.

d. **Biometrics.** Biometrics is an enabling tool that can be used as part of a multi-factor authentication process. As an authentication factor, biometrics leverage “something one is” (as opposed to “something one has” (e.g., a Personal Identification Verification card with Public Key Infrastructure (PKI) certificates) and “something one knows” (e.g., a Personal Identification Number (PIN)), and it cannot be shared or easily compromised. While biometrics first require an initial enrollment and thus cannot perform the role of initial identification, it can be used for continuing authentication in circumstances other than network access.