USE OF SOCIAL MEDIA

1. **REASON FOR ISSUE:** The Department of Veterans Affairs (VA) authorizes the use of social media tools to enhance communication and partner outreach. Using these tools supports VA and VA's goal of achieving improved employee effectiveness through seamless access to information. Social media tools enable widely dispersed facilities and agency users to effectively share information – which can result in better communication with Veterans, Service members and caregivers. The Office of Public and Intergovernmental Affairs (OPIA) and it's Office of Digital Media Engagement serves as functional lead for department-level digital media engagement and is responsible for establishing policies and procedures, as well as coordinating departmental digital media engagement processes and initiatives with VA Administration and VA Central Office Staff Office digital media efforts.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This Handbook establishes policy and provides guidance on the proper use of these tools, consistent with applicable laws, regulations, and policies. This Handbook supersedes policy and guidance related to the management of social media contained in VA Directive 6515, Use of Web-Based Collaboration Technologies.

3. **RESPONSIBLE OFFICE:** Office of Public and Intergovernmental Affairs (OPIA) (002).

4. **RELATED DIRECTIVE:** VA Directive 8500, Public Affairs, dated October 28, 2019.

5. **RESCISSION:** None.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Gary C. Tallman
Acting Assistant Secretary for
Public and Intergovernmental Affairs

DISTRIBUTION: Electronic Only

This page is intentionally left blank.

TABLE OF CONTENTS

USE OF SOCIAL MEDIA

1. PURPOSE.

a. This handbook provides policy guidance for the use of social media at the Department of Veterans Affairs (VA) and applies to official use of social media by agency users on behalf of VA for agency purposes, including public engagement and where indicated, to non-official or personal use of social media by employees. These two types of social media use are defined as:

(1) **Official Use:** Social media engagement on behalf of the agency and as authorized by the agency on sites where VA has an official web presence and terms of service agreement.

(2) **Non-Official/Personal Use:** Personal day-to-day use of social media sites by employees, not related to official duties. This includes use while on-duty or off-duty.

2. SCOPE.

a. This policy applies to the use of social media tools in which agency users represent the Department. The policy applies to all agency users designing, contributing, maintaining, using, or providing oversight of these tools. Agency Users include, but are not limited to, full-time and part-time employees, contractors, interns, and volunteers who access or contribute content.

b. Misuse of Government equipment/resources, non-compliance with or failure to follow agency policy, procedures, and guidance while using social media, or any other actions that violate applicable law, regulation, or policy may result in disciplinary action for Agency Users and other actions appropriate to their situation. Where indicated, this policy also applies to non-official or personal use by VA employees.

c. For the purposes of this handbook, “social media” covers tools and technologies that allow a social media user to share communications, postings or information, or participate in social networking, including but not limited to: blogs (e.g., X, Tumblr), social networks (e.g., Facebook, LinkedIn), video and photo sharing websites (e.g., YouTube, Instagram, Flickr), online forums and discussion boards, and automated data feeds for the purpose of educating and informing Veterans, their families, survivors, and caregivers.

d. This handbook does not assume responsibility for any mission, function, technology platform or procurement process, or the policy under the purview of the Assistant Secretary for Information Technology and Chief Information Officer.

3. POLICY.

a. It is VA policy that the organizations and program offices in the department use social media tools to enhance communication, information exchange, and internal/external engagement in accordance with applicable laws, regulations, and policies.

b. VA must comply with applicable Federal laws, regulations, and requirements including, but not limited to, Section 508 of the Rehabilitation Act of 1973, as amended in 1998, privacy, ethics, copyright, information security, and records management in its social media use.

c. Agency users and organizations engaged with these tools are responsible for ensuring that their use complies with applicable laws, regulations, and policies, including guidance from the Office of Management and Budget (OMB), and VA Directive 6102, Internet and Intranet Services, VA Directive and Handbook 6500, VA Cybersecurity Program, and this Handbook.

d. When used, VA entities will make social media tools available to agency users and organizations. Where access to social media sites may intrude upon business operations, local leadership will provide justification to the Assistant Secretary for Public and Intergovernmental Affairs when seeking to deny access social media to its agency users. Agency users and organizations will exercise sound judgment when using social media tools. The use of social media will promote the mission, goals and objectives of VA to educate and inform Veterans, their families, survivors, and caregivers. Such use shall be consistent with applicable laws, regulations and policy, as well as prudent operational, security and privacy considerations.

e. Agency users will maximize the quality, objectivity, utility, and integrity of the information provided to the public. As such, when officially representing the Department, Agency users will reasonably ensure that the agency position on a topic is properly represented in all communications. Articles and features about VA programs or initiatives that are intended for public release will follow VA policy.

f. Social media sites established for official VA use will be authorized, monitored, and moderated by the organizations hosting them. As the content owners, each administration, staff office, program office and facility is responsible for monitoring and maintaining all posted web content and assuring that the information is accurate and current. Additional policy and guidance is available in VA Directive 6102 and on the VA Social Media website.

g. VA's use of social media platforms will change over time as technology evolves. A list of approved platforms will be maintained on the VA Social Media website. These platforms will be managed using the enterprise-wide social media management tool authorized by both the Office of Public and Intergovernmental

Affairs and the Office of Information and Technology. No other tool may be used without written consent of both offices.

h. To establish an official VA social media account, the petitioner will develop a business case, have adequate resources to establish and maintain the site and ensure the organization's previously established channel(s) are up-to-date and meet VA quality standards.

i. OPIA is the final approving authority for all VA social media sites, except those of the Office of the Inspector General, which is exempt from this oversight and control per the Inspector General Act, 5 U.S.C. App. 3. However, OPIA may delegate approval or disapproval to administration communications offices.

j. A Web Page Privacy Policy (or link to the approved statement) will also be posted on the introductory page in accordance with VA Handbook 6502.3, Web Page Privacy Policy.

k. All VA social media pages or sites will contain the "Social Networking Disclaimer" found on the VA Privacy, Policies and Legal Information website. If the notice is not on the main page, the homepage will include a prominent link to the notice. In these cases, the marking will clearly identify the notice as "Privacy and Security - Legal Notice."

l. Agency users represent a rich source of information for Veterans. As such, agency users are encouraged to interact with the public online provided the interaction does not interfere with the performance of the remainder of their official duties. However, such activity comes with responsibility. When interacting with the public online, agency users will draw a clear distinction between their personal views and their professional duties. Agency users who are not officially authorized to speak on behalf of VA will never state or infer their communications represent VA's official position. Similarly, agency users should discourage Veterans and associated participants from seeking official VA determinations or adjudications via social media. In these cases, agency users will be clear that these requests will be submitted through the VA Social Media SharePoint site to ensure proper protection of personal information and for an official response to be provided.

m. Social media websites will not be used to monitor an individual's exercise of their First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of, an authorized law enforcement activity.

n. When it becomes necessary to officially contact individuals, VA employees shall generally not use social media outlets as an official mechanism for contacting individuals. To ensure continuity of access to all externally hosted, VA-sponsored social media tools, any account used by VA parties to disseminate official VA information shall be established using a VA shared email address.

Personal or individual VA email addresses will not be used to the extent practicable as a result of unique and varied social media tool platforms' terms of service.

o. Agency users will take appropriate action, in accordance with VA's social media disclaimer, on submissions by the public that contain vulgar language, personal attacks of any kind, offensive comments, libel, sensitive data and other inappropriate content.

4. RESPONSIBILITIES.

a. **Assistant Secretary for Public and Intergovernmental Affairs (AS/OPIA).** The AS/OPIA, as the designated senior agency official is responsible for web content and presentation, manages communications with Veterans, the public, VA employees and the news media. This responsibility includes coordination and distribution of the information VA communicates to any external audience, especially to the public through media and the provision of public affairs policy guidance for the Department. The AS/OPIA shall designate a Director of Digital Media Engagement as the official responsible for:

(1) Providing guidance on acceptable content for social media tools;

(2) Developing a strategy addressing the guidelines set forth within this policy that adheres to Federal guidelines on the use of social media;

(3) Reviewing, approving or disapproving requests by VA organizations to launch official social media presences;

(4) Setting content standards and disapproving any outward-facing content on official VA websites, blogs and social media sites that do not meet accepted standards of quality;

(5) Conducting periodic reviews of social media sites to ensure alignment with Department messaging and priorities and certify that those sites may continue to operate after audits are concluded; and

(6) Working with the appropriate VA Records Officer and the National Archives and Records Administration (NARA) to establish a Records Control Schedule (RCS) for VA records generated via VA social media that are not covered by an existing RCS.

b. **Assistant Secretary for Information and Technology and Chief Information Officer (CIO).** The CIO, as the senior agency official responsible for the Department's IT programs, is responsible for applying the requirements of this policy in its functions of providing appropriate agency-wide web technology services and security, policy, guidance and technical assistance to program offices.

c. **Office of General Counsel (OGC).** OGC provides legal advice to VA managers and leaders so they can work to support an effective civilian workforce for the Federal Government. In the context of social media, OGC provides legal guidance relating to the use of third-party and agency sponsored social media, use of the Web, terms of service agreements, ethics requirements for VA employees, privacy policies, and any other applicable matters.

d. **Director, VA Privacy Service.** In the context of social media, VA Privacy Service responsibilities include ensuring compliance with the Privacy Act of 1974, the privacy provisions of the E-Government Act of 2002, and other privacy-related laws, regulations, and guidance relating to the use of third-party and agency sponsored social media.

(1) **VA Records Officer.** VA Records Officer will work with content owners to ensure that all records generated through the use of social media adhere and conform to all documentation contained in the applicable RCS. Working with the Archivist of the United States and VA content owners, they will determine the most appropriate method(s) to capture and retain VA records hosted on both Federal servers and VA activities on non-Federal social media sites.

(2) **Assistant Secretaries and Other Key Officials (ASOKOs).** ASOKOs will appoint communications offices for each administration and staff office to be responsible for the following tasks, but may delegate to program and field office heads the responsibility to:

(3) Ensure that all externally-hosted social networking websites for programs under their control have a corresponding website located on a va.gov domain that is used as the official source for information pertaining to the subject presented on the externally-hosted website; and

(4) Designate a Social Media Manager (as defined on the Social Media website) to be accountable for any information dissemination on any official externally-facing VA social media sites which represent their respective organizational mission. (Note: While it is preferred that different people serve as social media coordinators and content manager(s), these roles may be combined if appropriate.)

(5) **Official VA Social Media Account Administrators.** VA officials within Administrations and Staff Offices designated by program managers as official VA Social Media Account Administrators will administer and run official VA social media accounts in a manner consistent with this social media policy, applicable law and related guidance. Administrators are responsible for controlling access to the account and maintaining account security (e.g., secure password maintenance and deactivating account access due to staffing changes).

(6) **Social Media Managers.** Social media managers will:

(a) Receive clearance from OPIA before launching any VA social media site;

(b) Consider the data protection aspects of their activity and in particular, whether it involves the transfer of VA sensitive information outside of VA;

(c) Use settings that allow for distinction between official VA postings and publicly-created content when they are available. Such settings should also:

i Allow VA-created content to be clearly delineated from that provided by the public;

ii Be optimized for VA's needs to communicate, distribute information and content, engage the public and capture new audiences through viral marketing. An example of this is the use of a Facebook "page" that will only allow for fans, as opposed to a Facebook "profile" that will allow for friends;

(d) Ensure that all social media websites for which they are responsible remain on topic and do not contain:

i Personal Identifiable Information,

ii Personal attacks of any kind,

iii Spam,

iv Language advocating illegal activity,

v Promotions of services, products, or political organizations,

vi Contain VA sensitive data, or

vii Clearly violates VA policy.

(e) Moderation of comments: the First Amendment greatly curtails enforcement of restrictions on free speech by a governmental entity. When the context of the speech is not clear, social media managers will give the benefit of the doubt to the commenter. However, the following are never allowed and can be deleted:

i Comments promoting drug or human trafficking,

ii Comments jeopardizing national security,

iii Child pornography,

iv Comments that incite violence,

v Defamation: potentially libelous comments.

(f) Ensure links remain current or discontinued when linked content is no longer available;

(g) Review all relevant content regularly as prescribed by OPIA or VA policy. Blogs and other social media sites remaining idle for 30 days (meaning no new content) may be removed, in accordance with the NARA requirements, at the discretion of OPIA or the Web Governance Board unless those idle periods are coordinated in advance;

(h) Answer questions posted to blogs and other social media sites by the public within a reasonable period of time or as prescribed by OPIA;

(i) Ensure that all information posted through social media is in accordance with VA Directive 0009, Ensuring Quality of Information Disseminated by VA;

(j) Request authority and receive clearance from OPIA and the appropriate administration communications offices before launching any social media site;

(k) Ensure that all VA blogs under their responsibility contain the “Social Networking Disclaimer;”

(l) Specific steps for Coordinators and Moderators to take for handling complaints will be outlined on the VA Social Media website.

(7) Agency Users.

(a) Any individual employed by the VA in a paid or unpaid position, including those appointed to full-time and part-time positions under title 5 or title 38, title 38 hybrid employees, individuals assigned to perform work for the VA under Intergovernmental Personnel Act agreements, temporary and intermittent employees, students, trainees, interns, volunteers and persons employed on a fee basis that have been authorized to use official VA social media sites as part of their official duty.

i When acting in their official capacities, agency users are responsible for the content they publish on blogs, wikis or any other form of user-generated media. Published information will be public for a long time.

ii When interacting on blogs, wikis, social networks, virtual worlds and social media, agency users shall:

(A) Never comment on VA mission-related legal matters unless they are VA's official spokesperson for the matter and have management approval to do so;

(B) Be professional at all times when posting to VA-related social media and use their best judgment when interacting on social media about matters related to VA's mission;

(C) In their capacities as VA representatives, post only information about which they have actual knowledge. Never comment or provide information on any matter about which they do not have actual, up to date knowledge;

(D) Identify themselves and their roles as VA representatives when commenting or providing information on matters related to VA's mission;

(E) Be aware of their associations with VA in online social networks. If they identify themselves as VA representatives, ensure that their profiles and any related content is consistent with how they wish to present themselves to colleagues, members of the Executive and Legislative Branches of the Federal Government and the public;

(F) Never post information protected by the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Act of 1974, 38 U.S.C. §§ .5701, 5705, or 7332, or VA policy on any digital collaboration tool without legal authority and prior approval by authorized official and unless proper, VA approved security measures are in place. All agency users will have access as appropriate for the performance of their official VA duties;

(G) Never use profanity, make libelous (or defamatory) statements, use privately-created works without the express, written permission of the author, or quote more than short excerpts of other people's work;

(H) Only post and use content in accordance with applicable ethics, intellectual property, records and privacy laws, regulations and policies;

(I) Use Government Office Equipment including IT in accordance with VA Directive 6001, Limited Personal use of

Government Office Equipment Including Information Technology and;

(J) Use only direct messaging services approved by VA as found on the Social Media Guidance website

5. RESTRICTIONS FOR SOCIAL MEDIA USE.

a. All VA employees are required to comply with the below restrictions that apply to online communications at all times, regardless of whether they are at work, outside the office, or using government equipment. The restrictions on VA employee communications are contained in statutes, the Code of Federal Regulations (C.F.R.) and current agency policies. For example, when using social media tools and third-party sites for either official or personal use, VA employees are bound by the Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. part 2635.

b. While not exhaustive, the following restrictions apply to all employees, and violations may be cause for disciplinary action by the agency (Note that The Office of Government Ethics (OGE) published Legal Advisory 23-03, The Standards of Conduct and **18 U.S.C. § 208** as Applied to Official Social Media Use. This advisory provides in-depth analysis with examples.):

(1) **Criminal or Dishonest Conduct:** Employees will not engage in criminal or dishonest conduct.

(2) **Conflict of Interest:** A Federal employee may not participate personally and substantially in a particular VA matter that will directly affect an employee's own financial interest or the financial interests of those persons and entities whose financial interests are imputed. 18 U.S.C. § 208. Additionally, employees are required to act impartially and not give preferential treatment to any private organization or individual. 5 C.F.R. § 2635.101(b)(8).

(3) **Misuse of Position:** Employees will not use their public office for private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or other acquaintances. Also, employees will not use or permit the use of their government position or title or any authority associated with their public office in a manner that is intended to coerce or induce another person to provide any benefit, financial or otherwise, to themselves or to friends, relatives, or persons with whom the employees are affiliated in a nongovernmental capacity. Finally, with limited exceptions (See 5 C.F.R. § 2635.702(b), (c)) employees will not use their government position or title in a manner that could reasonably be construed to imply that the Government endorses or sanctions their personal activities or those of another. 5 C.F.R. § 2635.702.

(4) **Use of Government Time and Property:** When employees are on duty, the Standards of Ethical Conduct require that they use official time in an honest effort to perform official duties (see 5 C.F.R. § 2635.705). The Standards of Ethical Conduct also require employees to protect and conserve Government property and to use Government property only to perform official duties, unless they are authorized to use government property for other purposes (see 5 C.F.R. § 2635.704). For example, under the Standards of Ethical Conduct, a supervisor may not order, or even ask, a subordinate to work on the supervisor's personal social media account. Coercing or inducing a subordinate to maintain the supervisor's personal account would amount to a misuse of position and, if done on official time, a misuse of official time. The same would be true if the supervisor were to have a subordinate create content for the supervisor's personal account, even if the subordinate were not involved in uploading the content to that account (5 C.F.R. §§ 2635.702(a), 2635.705(b)). Employees should report such matters to the designated agency ethics officer. The duty to protect and conserve Government property also extends to preventing unauthorized access and use of official accounts by non-authorized persons, including former employees. Federal employees who oversee official social media accounts are responsible for protecting those assets and preventing unauthorized use. As a result, former employees are restricted from using the official social media accounts of the VA after their departure.

(5) **Use of Non-Public Information:** Employees will not allow the improper use of nonpublic information to further their private interest or that of another, whether by engaging in financial transactions using such information, through advice or recommendation, or by knowing unauthorized disclosure. Non-public information is information that the employee gains by reason of Federal employment and that they know or reasonably should know have not been made available to the public (5 C.F.R. § 2635.703). Furthermore, employees will not make careless or intentional unauthorized disclosures of nonpublic information, unless disclosure is authorized by law. Other unauthorized disclosures include, but are not limited to, the unauthorized dissemination of classified information, proprietary information, and the content of confidential and deliberative discussions. A criminal statute, 18 U.S.C. § 1905, protects and prohibits the use or disclosure of trade secrets and confidential business information.

(6) **Political Activity:** Employees must avoid engaging in certain types of political activity, including activity on social media, that is prohibited by the Hatch Act, 5 U.S.C. §§ 7321-7326. The U.S. Office of Special Counsel has posted a guidance document and chart regarding when Federal employees' use of social media could violate the Hatch Act. For further guidance regarding the Hatch Act's prohibitions or questions about how the

Hatch Act might apply to a VA planned use of social media, please contact the VA's Ethics Specialty Team.

(7) **Grassroots Lobbying:** VA annual appropriations authorizations prohibit the use of appropriated funds for indirect or grassroots lobbying in support of or in opposition to pending legislation. Agency users authorized to use social media in their official capacity must not post content on behalf of VA that includes requests to contact a member of Congress, a jurisdiction, or an official of any Government entity (Federal, state, or local) to favor or oppose any legislation, law, or appropriation because such grassroots lobbying activities are prohibited by Federal law.

(8) **Discrimination and Harassment:** All employees have a responsibility to maintain an appropriate level of professional conduct in the workplace, and to treat fellow employees with respect and fairness. Pursuant to the VA Harassment Prevention Policy, VA prohibits harassing conduct (sexual or non-sexual) in any VA workplace or in any work-related situation at any other location during or outside normal duty hours. VA also prohibits retaliation against an employee who alleges harassment or who assists in any inquiry related to allegations of harassment. Additionally, VA does not tolerate unlawful discrimination, workplace harassment or retaliation based on race, color, religion, national origin, sex (including gender identity, transgender status, sexual orientation, and pregnancy), age (40 or older), disability, or genetic information, marital status, parental status, political affiliation or retaliation for opposing discriminatory practices or participating in the discrimination-complaint process. VA also prohibits discrimination based on sexual orientation, marital status, political affiliation, parental status, military services or any other non-merit factor. See 5 U.S.C. §§ 2301- 2302 (prohibited personnel practices).

(9) **Children:** Agency Web sites or social media accounts must not collect any personal information from children (under the age of 13) in violation of the Children's Online Privacy Protection Act. 15 U.S.C. §§ 6501-6505.

(10) While VA encourages the use of social media disclaimers on personal sites, employees are not exempt from administrative or disciplinary actions due to content or comments made or shared by an employee on their personal site and personal time that can be considered racist, sexist, or discriminatory against any class of protected persons, or otherwise detracts from one's character or reputation. VA employees retain First Amendment rights to speak on matters of public concern, however, personal conduct that affects the efficient operation of any VA office, creates actual or potential disruption to the workplace, or otherwise affects the accomplishment of VA's mission may be grounds for adverse actions and possible termination of employment.

6. REFERENCES.

a. Age Discrimination in Employment Act, 29 U.S.C. §§ 621.

b. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505.

c. Copyright Act, 17 U.S.C. Ch. 1-13

d. Disposal of Records, 44 U.S.C. Ch. 33

e. Electronic Records Management, 36 C.F.R. Part 1236

f. Freedom of Information Act (FOIA), as amended, 5 U.S.C. § 552

g. GAO Decision, Environmental Protection Agency--Application of Publicity or Propaganda and Anti-Lobbying Provisions, B-326944, (Dec. 14, 2015).

h. HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164.

i. The Lanham Act, 15 U.S.C. Ch. 22.

j. Legal Advisory 23-03, The Standards of Conduct and **18 U.S.C. § 208** as Applied to Official Social Media Use.

k. OMB Memorandum M-10-06, Open Government Directive (Dec. 8, 2009).

l. OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).

m. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).

n. OMB Memorandum M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements (April 4, 2013).

o. OMB Memorandum, Social Media, Web-based Technologies, and the Paperwork Reduction Act, April 7, 2010.

p. NARA Bulletin 2014-02, Guidance on Managing Social Media Records, October 25, 2013.

q. Political Activities of Federal Employees, 5 C.F.R. part 734

r. Privacy Act of 1974, 5 U.S.C. 552a,.

s. Safeguarding Personal Information In Department of Veterans Affairs Records, 38 C.F.R. §§ 1.575 – 1.584

t. Prohibited Personnel Practices 5 U.S.C. §§ 2301- 2302.

u. Records Management by the Archivist of the United States, 44 U.S.C. Ch. 29

v. Rehabilitation Act of 1973 (Pub. L. 93-112), *29 U.S.C. 501, et seq.*

w. Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. part 2635

x. The Hatch Act, 5 U.S.C. §§ 7321-7326

y. Title VII of the Civil Rights Act of 1964, as amended.

z. U.S. Office of Government Ethics: LA-15-03 The Standards of Conduct as Applied to Personal Social Media Use (April 9, 2015).

aa. VA Directive 0009, Ensuring Quality of Information Disseminated by VA.

bb. VA Directive and Handbook 5979, Harassment Prevention Policy.

cc. VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

dd. VA Directive 6102, Internet and Intranet Services.

ee. VA Directive 6221, Accessible Electronic Communications Technology.

ff. VA Directive 6300, Records and Information Management.

gg. VA Directive 6371, Destruction of Temporary Paper Records.

hh. VA Directive 6502, VA Enterprise Privacy Program.

ii. VA Directive 6515, Digital Medial Collaboration Tools

jj. VA Handbook 6502.3, Web Page Privacy Policy.

7. DEFINITIONS.

a. **Agency User**. The term agency user includes VA employees, volunteers, interns, and contractors that have been authorized to use official VA social media sites as part of their official duty.

b. **Individual.** The term individual includes employees of VA, volunteers, VA contractors, VA beneficiaries and their dependents or survivors and others with whom VA has a business relationship and collects or stores social security numbers.

c. **Personally Identifiable Information.** Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or

identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

d. **Social Media.** "Social Media" are web-based tools, websites, applications and media that connect users and allow them to engage in dialogue, share information and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users.

e. **VA Sensitive Information or Data.** All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under FOIA.

f. **Vulgar Language.** Lewdly or profanely indecent language.