DEPARTMI **8320-01**

38 CFR Part 0

RIN 2900-AR52

Principle-based Ethics Framework for Access to and Use of Veteran Data

AGENCY: Department of Veterans Affairs.

ACTION: Final rule.

SUMMARY: The Department of Veterans Affairs (VA or Department) amends its regulations concerning the standards of ethical conduct and related responsibilities of its employees by adopting an overarching principle-based ethics framework for access to and use of veteran data. This framework is an important part of VA's data governance strategy. A data ethics framework can ensure uniform ethics standards for data practices and address consumer protection and data stewardship concerns that are beyond traditional privacy and confidentiality practices. This framework is intended to be applied by all parties who oversee the access to, sharing of, or the use of veteran data, or who access, share, or use veteran data themselves in the context of all other specific clinical, technical, fiscal, regulatory, professional, industry, and other standards.

DATES: This final rule is effective **[insert date of publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT: Kenneth Berkowitz MD FCCP, Special Advisor, VHA National Center for Ethics in Health Care (10ETH), Department of Veterans Affairs, Veterans Health Administration, 810 Vermont Ave. NW, Washington, DC 20420. 202-632-8457. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION: Federal statutes and regulation establish parameters for accessing, sharing, and use of data collected by Federal and state agencies as well as non-governmental organizations and institutions. Limitations on accessing, sharing, or use of data varies based on what type of data is collected. Various Federal laws require or permit disclosure or sharing of data under specific circumstances.

While law, regulation, and policy set important standards for data access, sharing, and use, they do not always provide definitive guidance about how VA should manage access, sharing, or use of veteran data when regulation and policy permit organizational discretion. Given burgeoning access to, sharing of, and use of VA data, proceeding without establishing clear expectations for access to, sharing of, and use of VA data is a disservice to veterans, the Department, and our partners, and creates a serious risk due to inconsistent or problematic data access, sharing, or use. These risks could undermine our imperative to harness the tremendous potential of VA data to support and improve veteran health and wellness; the delivery of services to veterans; and overall public health. VA has adopted an overarching principle-based ethics framework for access to, sharing of, and use of veteran data which is the subject of this rulemaking. This framework is an important part of VA's data governance strategy. A data ethics framework ensures uniform ethics standards for data practices and addresses concerns that are beyond traditional privacy and confidentiality practices.

This data ethics framework is intended to be applied by all parties who oversee the access to, sharing of, or the use of veteran data, or who access or use veteran data themselves in the context of all other specific clinical, technical, fiscal, regulatory, professional, industry, and other standards.

In brief, the Ethical Framework Principles for Access to and Use of Veteran Data, explained in further detail in regulation, are as follows:

Principle 1. The primary goal for use of veteran data is for the good of veterans. Veteran data is personal and sensitive.

Principle 2. Veteran data should be used in a manner that ensures equity to veterans.

Principle 3. The sharing of veteran data should be based on the veteran's meaningful choice.

Principle 4. Access to and exchange of veteran data should be transparent and consistent.

Principle 5. De-identified veteran data should not be reidentified without authorization.

Principle 6. There is an obligation of reciprocity for gains made using veteran data.

Principle 7. All parties are obligated to ensure data security, quality and integrity of veteran data.

Principle 8. Veterans should be able to access to their own information.

Principle 9. Veterans have the right to request amendments to their own information.

Administrative Procedure Act

The Administrative Procedure Act provides that the general requirement that notice and opportunity for public comment does not apply to a matter relating to agency management or personnel, rules of agency procedure or practice, or general statements of policy. 5 U.S.C. 553(a)(2) and (b)(3)(A). The Secretary finds that this rulemaking

concerning VA's data ethics framework for access to and use of veteran data relates solely to agency procedure or practice and is a general statement of policy and is exempt from notice and comment provisions of the Administrative Procedure Act. For the same reason, this rule is also exempt from the delayed effective-date requirement in 5 U.S.C. 553(d).

Paperwork Reduction Act

This final rule contains no provisions constituting a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521).

Regulatory Flexibility Act

The Secretary hereby certifies that this final rule does not have a significant economic impact on a substantial number of small entities as they are defined in the Regulatory Flexibility Act, 5 U.S.C. 601-612. The provisions of this rulemaking have no economic and/or monetary impact. VA is merely establishing an overarching ethical framework and principles to adhere to when managing, accessing and usage of veteran data. Therefore, pursuant to 5 U.S.C. 605(b), the initial and final regulatory flexibility analysis requirements of 5 U.S.C. 603 and 604 do not apply.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic,

environmental, public health and safety effects, and other advantages; distributive impacts; and equity). Executive Order 13563 (Improving Regulation and Regulatory Review) emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. The Office of Information and Regulatory Affairs has determined that this rule is not a significant regulatory action under Executive Oder 12866. The Regulatory Impact Analysis associated with this rulemaking can be found as a supporting document at www.regulations.gov.

Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 requires, at 2 U.S.C. 1532, that agencies prepare an assessment of anticipated costs and benefits before issuing any rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. This final rule has no such effect on State, local, and tribal governments, or on the private sector.

Assistance Listing

There are no Assistance Listing numbers and titles for the programs affected by this document.

Congressional Review Act

Pursuant to the Congressional Review Act (5 U.S.C. 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a major rule, as defined by 5 U.S.C. 804(2).

List of Subjects in 38 CFR Part 0

Conflict of interests.

Signing Authority

Denis McDonough, Secretary of Veterans Affairs, approved this document on June 30, 2022, and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.

***Consuela Benjamin**,*

Regulations Development Coordinator,
Office of Regulation Policy & Management,
Office of General Counsel,
Department of Veterans Affairs.

For the reasons set forth in the preamble, the Department of Veterans Affairs amends 38 CFR part 0 as follows:

PART 0 – VALUES, STANDARDS OF ETHICAL CONDUCT, AND RELATED RESPONSIBILITIES

1. The authority citation for part 0 continues to read as follows:

Authority: 5 U.S.C. 301; 38 U.S.C. 501; see sections 201, 301, and 502(a) of E.O. 12674, 54 FR 15159, 3 CFR, 1989 Comp., p. 215 as modified by E.O. 12731, 55 FR 42547, 3 CFR, 1990 Comp., p. 306.

2. Add § 0.605 to read as follows:

§ 0.605 Ethical framework principles for access to and use of veteran data.

(a) Veterans trust VA to promote and respect their privacy, confidentiality, and autonomy in the services we provide or support. We earn this trust when we adhere to VA's core values of integrity, commitment, advocacy, respect, and excellence (commonly referred to as ICARE).

(b) Consistent with the values listed in paragraph (a) of this section, VA must promote and ensure responsible practices whenever veteran data is accessed, shared, or used by VA or its partners. Veteran data is accessed, shared, and used for many purposes which are developing at an unparalleled pace. While the regulatory and policy framework that governs data access, sharing, and use sets important standards about what is required with respect to data access, sharing, and use, it does not always provide definitive guidance about how VA should manage access, sharing, or use of veteran data when regulation and policy permit organizational discretion, except in cases where there are already established federally protected classes.

(c) The following principles establish an overarching ethical framework for all individuals, groups, or entities to apply when managing access to, sharing of, or use of VA veteran data. All parties who have or obtain access to and use VA veteran data are encouraged to carefully consider and apply this principle-based ethical framework when not contradicted by other specific clinical, technical, fiscal, regulatory, professional, industry, and other standards. VA and its partners must apply this principle-based ethical framework when accessing, sharing or using veteran data unless prohibited by law. Consistent application of this framework will ensure the integrity and trustworthiness that veterans and other stakeholders expect and deserve when veteran data is accessed, shared, or used.

(1) Principle 1. The primary goal for use of veteran data is for the good of veterans. Veteran data is personal and sensitive. Use of veteran data by VA and its partners must have the primary goal of supporting and improving overall veteran health and wellness, and the delivery of benefits and services to veterans at large.

(2) Principle 2. Veteran data should be used in a manner that ensures equity to veterans. The proper use of veteran data by VA and its partners must help to ensure equity so that no veteran population is disproportionally excluded from the benefits of, or burdened by the risks of, data use because of race, color, religion, national origin, limited English proficiency, age, sex (including gender identity and transgender status), sexual orientation, pregnancy, marital and parental status, disability, or genetic information.

(3) Principle 3. The sharing of veteran data should be based on the veteran's meaningful choice. When regulation and policy permit organizational discretion, the sharing of veteran data by VA and its partners should be based on the veteran's meaningful choice to permit sharing their information for that specific purpose;

exceptions for sharing based on a veteran's meaningful choice are treatment, payment, health care operations, public health and safety reporting, and when required by law. Timely, clear, relevant, concise, complete, and comprehensible information must be provided to the veteran to serve as a basis for their free and informed choice. A veteran's preference to change their mind about sharing or not sharing their information should be facilitated, with the understanding that information that has already been shared may be unable to be retrieved or retracted. A veteran's choice(s) about data sharing must not be the basis to deny care or benefits to which they are otherwise entitled. Meaningful choice may be expressed in many forms and a written requirement is not implied.

(4) Principle 4. Access to and exchange of veteran data should be transparent and consistent. Access to and the exchange of veteran data should be transparent and consistent, and in accordance with all applicable standards. For the Veterans Health Administration (VHA), this includes practices described in VHA's Notice of Privacy Practices. Data should only be shared or accessed for approved and specified purposes; there should be no un-specified use, or re-use of veteran data without VA agreement or approval. The release of veteran data for purposes other than those which were originally approved or specified, such as in an agreement, requires a separate approval and commitment of all parties to follow these principles. Failure to ensure such protections is a breach of veteran trust and confidentiality.

(5) Principle 5. De-identified veteran data should not be reidentified without authorization. Parties who receive de-identified veteran data must not attempt to re-identify the data in any manner without prior VA agreement or approval. VA considers unauthorized re-identification a breach of veteran trust and confidentiality.

(6) Principle 6. There is an obligation of reciprocity for gains made using veteran data. A financial or other gain from innovation by non-VA parties that uses veteran data obtained from VA creates a moral and tangible obligation of reciprocity to share this gain with veterans, veterans' service organizations, and/or veterans' causes. For example, parties could fulfill this obligation by giving back to the veteran community through support of veteran causes or organizations, by facilitating veteran access to innovations to which veteran data contributed, or, at a minimum, by publicly recognizing veteran contributions to the gain or innovation. Veteran data must not be sold by VA or its partners.

(7) Principle 7. All parties are obligated to ensure data security, quality and integrity of veteran data. All parties who send, receive, or use VA veteran data must ensure data security, quality, and integrity. In other words, that the data remain secure; accurate; complete; and representative of the data quality, meaning, and integrity when it was received or accessed from VA. Access to data by VA and its partners should be limited to the minimum amount needed to accomplish the stated purpose and should be terminated when no longer required. Data that are not necessary to accomplish the purpose for which it was obtained should not be retained longer than legally required. Transparency about breaches in data security, quality or integrity is also essential to promote trust and minimize impacts to veterans.

(8) Principle 8. Veterans should be able to access to their own information. Veterans must have user-friendly access to their own information. Access may be through electronic means such as mobile applications, web portals, or through convenient written or in-person processes.

(9) Principle 9. Veterans have the right to request amendments to their own information. Veterans must be able to request amendments to information in their VA records if they feel it is untimely, inaccurate, incomplete, or not relevant.

(d) As used in this section, *de-identified veteran data* means information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information is individually identifiable information or can be used by any means to identify an individual. For protected health information (PHI), veteran data is not de-identified unless in compliance with 45 CFR parts 160 and 164.

[FR Doc. 2022-14437 Filed: 7/6/2022 8:45 am; Publication Date: 7/7/2022]