WDVA/CVSO/TVSO VBATS Access Login Agreement

THIS AGREEMENT for Release of Confidential Veterans Information is agreed to and made upon the successful login access of the VBATS Application by the VBATS user (hereinafter "Access User/Receiving Party") and between the state of Wisconsin, Department of Veterans Affairs, (hereinafter "WDVA" or "Disclosing Party"). Note, the Access User/Receiving Party represents and warrants to WDVA that the Access User/Receiving Party has authority to bind the User/Receiving Party's underlying organization (e.g., County, Nation, or CVSO Office) and that any access or use of VBATS by the Access User/Receiving Party constitutes an automatic renewal of the signed Memorandum of Understanding between WDVA and the User/Receiving Party's underlying organization, Additionally, any continuing use binds not only the User/Receiving Party to both the signed agreement and the terms below, but also, User/Receiving Party's underlying organization.

Background

1. WDVA is a state agency created under the provisions of Chapters 15 and 45, Wisconsin Statutes, whose mission is to give health, educational, and economic assistance to Veterans and their dependents who are residents of this state;.
2. WDVA is the recipient of the United States Department of Defense service records and other information provided by the U.S. Department of Veterans Affairs (hereinafter referred to as "VA") which are considered to be confidential pursuant to Title 38 United States Code and Wis. Stat. § 45.04(3).
3. The Access User/Receiving Party is a Wisconsin County or Tribal Veterans Service Office user of the VBATS application, authorized to receive confidential information pursuant to Wis. Stat § 45.04, and the Wisconsin Administrative Code, § VA 1.10.
4. The Access User/Receiving Party has demonstrated the need to receive Veterans' confidential information in order for Access User/Receiving Party to continue to provide information and services related to Veteran's benefits.
5. The intent of this agreement is twofold; (1) to allow the Access User/Receiving Party access to the WDVA Veterans Benefit Application Tracking System (VBATS) database without restriction and remove the requirement for release forms signed by the Veteran, dependents, survivors, or duly authorized representatives (excepting current and former WDVA staff); and (2) to protect the confidentiality, integrity, and availability of information created, processed, stored, aggregated, and transmitted by the Disclosing Party.
6. The Disclosing Party and the Access User/Receiving Party wish to discuss and exchange information related to benefits for Veterans and their dependents, which the parties hereto and applicable regulatory bodies as part of their joint missions and partnership in serving Veterans, consider highly confidential, while at the same time ensuring full compliance with applicable state and privacy laws.
7. Access User/Receiving Party's access under this Memorandum and other benefits include:
    A. Statewide access to VBATS records
    B. Ability to "add" and "upload documents", to include discharge documents, in VBATS without WDVA verification.
    C. View VBATS Veteran records without a Request for Release of Records (Form 1042), except for WDVA former/current employee VBATS records.
    D. Elimination of the annual requirement to submit a VBATS Account Authorization Request Form to maintain access to VBATS.
    E. Access to Recently Separated Veterans contact information/report in VBATS.
    F. Access to the Department of Defense Personnel Records Retrieval System (DPRIS) for DD214 information (with DoD approval)
    G. Access to the following reports on a statewide basis:
        1. Death Report by County or Cemetery Report;
        2. Grave Registration Activity Report;
        3. County Applications List Report;
        4. County Initiated Applications Report;
        5. DMDC DD214 Report;
        6. County Benefits Report; and
        7. Museum Veteran Search.

8. Access User/Receiving Party's Obligation of Compliance: Access User/Receiving Party, under penalty of perjury, agrees to ensure full Compliance with Privacy Laws. To include, but not limited to, the following: USDVA Policies - VHA Handbook 1605.1, Privacy & Release of Information, VA Directive 6504, "Restrictions, Transportation & Use of & Access to VA Data Outside of VA Facilities;" VA IT Directive 06-02, "Safeguarding Confidential & Privacy Act-Protected Data at Alternative Work Locations;" VA IT Directive 06-06, "Safeguarding Removable Media;" & VA Memorandum, February 6, 2007; Wis. Stat. §§ 45.04 (DVA records privacy), 146.82 – 146.83 (protected health information), 610.70 (Disclosure of Personal Medical Information); WI Admin. Code: DHS 92 (Confidentiality of Treatment Records); 5 U.S.C. § 552a (Privacy Act); USDVA Privacy Policies; 38 U.S.C. 5701; 38 U.S.C. 7332; The Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule, 45 Code of Federal Regulations Parts 160 & 164; Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705; OMB Memorandum M-07-16, Safeguarding Against & Responding to Breach of Personally Identifiable Information, May 22, 2007; DoD Memorandum: Safeguarding

Against & Responding to Breach of PII, 21 Sep, 2007; DoD 5400.11-R: DoD Privacy Program, 14 May, 2007; and DoD Directive 5400.11, DoD Privacy Program, 8 May 2007.

Any use or access of the WDVA VBATS system constitutes a binding and enforceable agreement to the following terms and conditions of use:

I. Definitions.

A. **"Veteran"** shall mean an individual that meets the definitions contained in Wis. Stat. §§ 45.001, 45.01(12), 45.02, 45.43(1), 45.51 (2)(a)1, and 45.51(2)(a)2, 45.61(2).

B. **"Confidential, Sensitive and/or Protected Information (collectively hereinafter referred to as 'PI')"** shall include all forms of personally or individually identifiable information, personally identifiable health information, sensitive information, information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection, and all information related to the Veteran provided by Disclosing Party to Access User/Receiving Party as further defined by VA DIRECTIVES 6509, Provision 5 and VA Handbook 6500, and successor directives and handbooks pertaining to these definitions published by the U.S. Department of Veterans Affairs. PI shall also mean all information provided by Disclosing Party with respect to the Veteran regardless of whether it is written, oral, contained on various storage media, or human or machine-readable documents.

C. **"Data Breach"** shall mean the loss, theft, or any other unauthorized access, other than that incidental to the scope of employment, to data containing PI in electronic or printed form which results in the compromise of the confidentiality or integrity of the data.

D. **"Maintain"** shall mean to collect, create, use, process, store, disseminate, transmit, or dispose of PI.

II. **Legal Obligation to Safeguard Veteran Data.** Each party is individually responsible for determining which laws apply to their respective organizations, and for ensuring compliance. A non-exhaustive list of current laws which apply to the type of data provided by WDVA under this Agreement; including the following:

A. Provisions of law directly related to VA Claims:
   1. 38 U.S.C. § 5701 Confidential Nature of Claims (USDVA claims confidentiality):
      a. Provides for the confidentiality of all VA patient claimant information, with special protection for their names and home addresses.
      b. Provides for the same for information about their dependents.
      c. Prohibits disclosure of these names and addresses except as authorized by the statute.
      d. Does not apply to employee information.
   2. VHA Handbook 1605.1, Privacy and Release of Information, establishes guidance on privacy use and disclosure of PI. This handbook (link below) provides guidance as to the legal obligations relative to federal law, applicable to the Claims Staff: http://www1.va.gov/vhapublicationsNiewPubfication.asp?pub_ID=1423.

B. Veterans' personal data may also be protected by the following provisions of law. All parties must follow appropriate procedures to safeguard the privacy of Veterans' personal data.
   1. **State Law:**
      a. Wis. Stats. § 19.80(3)(a);
      b. Wis. Stats. § 45.04;
      c. Wis. Stats. § 106.01;
      d. Wis. Stats. § 134.97;
      e. Wis. Admin. Code § 296.01; and
      f. Wis. Admin. Code § VA 1.10.
   2. **Federal Law and Guidance:**
      a. 38 C.F.R. § 1.500;
      b. 38 U.S.C. § 7332;
      c. 38 C.F.R. §§ 14.626-14.637;
      d. 38 C.F.R. §§ 75.111-119;
      e. 38 U.S.C. § 5721 et seq.;
      f. 38 U.S.C. § 3672;
      g. Privacy Act of 1974, 5 U.S.C. § 552a;
      h. To the extent Access User/Receiving Party is subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191 and its implementing regulations at 45 C.F.R. parts 160 and 164; and HIPAA/HITECH Act Omnibus Final Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013) and section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C.§ 17932) Breach Notification Rule at 45 C.F.R. §§ 164.400-414 as independently determined in consultation with corporation counsel,

Office of Management and Budget (0MB) Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;

i. VA Directive and Handbook 0710, Personnel Suitability and Security Program;
j. VA Directive 6500, Manage Information Security Risk: VA Information Security Program;
k. VA Handbook 6500, Risk Management Framework tor VA Information Systems, Tier 3: VA Information Security Program;
l. VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information;
m. VA Directive 6502, VA Enterprise Privacy Program;
n. VA Handbook 6502.1, Privacy Violation Tracking System (PVTS), the Formal Event Reporting and Evaluation Tool (FERET) guidebook;
o. VHA Directive 1605, VHA Privacy Program;
p. VHA Handbook 1605.1, Privacy and Release of Information;
q. VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information; and
r. Memorandum from Office of General Counsel (02) to Under Secretary for Health (10), "Request for Advisory Opinion - Department Information Ownership." dated December 31, 2007.

III. Use of PI.

A. The parties agree:

1. **Privacy Right. Except as otherwise required by law,** the privacy of PI shall beprotected in all functions, services, and facilities.
2. VBATS Account Authorization.
   a. To gain access and to login to the VBATS, the Access User/Receiving Party must register an account utilizing the VBATS login link, and submit a VBATS Account Authorization Request (WDVA Form 2419) to WDVA for each county employee seeking access to ensure that access is authorized to utilize the VBATS for WDVA programs and benefits. Multiple County employees can be included on each WDVA Form 2419. Completed forms can be emailed to WDVA at sysdevrequest@dva.wisconsin.gov The WDVA Form 2419 must be received and approved by WDVA before VBATS access or login is granted to the Access User/Receiving Party. Notification to the Access User/Receiving Party shall be emailed once approved.
   b. The corporation counsel of Access User/Receiving Party or the Access User/Receiving Party shall notify WDVA upon his or her notice that an authorized user shall terminate employment. Notification shall be sent utilizing the Replace Field on a WDVA Form 2419 and sent via email to sysdevrequest@dva.wisconsin.gov . This is to ensure privacy and security by disabling user access to only authorized employees of Access User/Receiving Party.
   c. Access to VBATS records of former or current WDVA employees requires a signed Request for Release of Military Separation Records And Personal Information to the County or Tribal Veterans Service Office Form (WDVA 1042) from said employee granting access on file at WDVA.
3. **Annual Review.** Each party shall review applicable privacy and security safeguards that are in place to protect PI on a reasonable basis and within 30 days of any confirmed security breach. PI shall be maintained in a manner that shall ensure legal compliance with federal and state statute, laws, rules and guidelines as determined appropriate by each party in consultation with each party's respective legal counsel.
4. **PI shall be kept confidential.** In accordance with 5 U.S.C. 552a, 38 U.S.C. §§ 5701, 5705, and 7332, and other applicable federal privacy laws and regulations, as appropriate, parties shall ensure that all PI that is maintained in any medium, is kept confidential, except when disclosure is permitted or compelled under law.
5. PI shall **be properly controlled.** All PI in the custody and control of each party shall be used and disclosed only as permitted or required by law.
6. **Contractor-controlled PI shall be properly maintained.** Parties shall ensure that all contracts in which any data containing WDVA-owned PI or Veteran PI that is maintained by contractors shall contain the appropriate clauses as may be required by law.
7. **Data shall be protected.** The physical input and output products of WDVA information and systems that contain PI, such as disks, paper, flash drives or any other data storage devices, shall be protected against misuse and unauthorized access, unauthorized disruption, unauthorized disclosure, or unauthorized modification or destruction. No technology utilized to collect, use, or disclose PI shall erode privacy protections afforded by applicable state or federal law or WDVA policy.
8. **PI shall be kept secure.** Security plans shall be continually developed and security controls implemented on all networks and filing systems that maintain PI in any form. These controls shall be implemented, as required by applicable law or policy, to, among other things, protect the security and privacy of all operating or filing systems used to access or store PHI, application software used to access or store PHI, and data in WDVA information systems. The purpose of these plans is to prevent the accidental or malicious disclosure, alteration or destruction of PI, and to provide assurances to the user of the quality, integrity, and confidentiality of such information maintained by the parties. Technologies used to maintain this information should allow for continuous auditing of compliance with this Agreement.
   a. **Privacy and data breaches shall be reported.** Parties shall report all breaches by their personnel, contractors, and authorized users involving PI in a timely and complete manner, as required by applicable law to the WDVA Privacy Officer as soon as possible but no later than within (five) 5 business days of discovery. The party at fault shall resolve all such breaches with privacy implications in a timely fashion in accordance with applicable law and policy. For further guidance, see VA Handbook 6502.1, Privacy Violation Tracking System (PVTS), the Formal Event Reporting and Evaluation Tool (FERET) guidebook, and VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information.
   b. **The data breach process shall be sustained.** Each Party shall maintain a process for the tracking and reporting of suspected or actual breaches involving PI in compliance with the references above.
9. **Training.** The WDVA Privacy/Security Officer, or WDVA cornerstone training through the HR Star portal, shall be available to provide at minimum, annual privacy awareness training to WDVA employees, and if requested by the Access User/Receiving Party on reasonable notice and accommodation of schedules,

WDVA shall provide access to training modules or PowerPoint presentations.

B. Rules for Electronic Communications:

1. Parties acknowledge email messages sent by or to their offices may be read by someone other than the person to whom they are sent and may have to be disclosed to outside parties or in court in connection with a lawsuit. Accordingly, each party must take care to ensure that their messages are courteous, professional, and that the tone and words they use would not cause embarrassment to themselves or their organization if the message were made public.
    a. Any email sent outside each party's network or information system should be considered non-secure.
    b. Email is subject to applicable privacy, security, and records retention laws and guidelines for the information that particular message contains. As such, email records must be appropriately secured and retained.
2. Each party is responsible for the content of all text, audio or images that they place or send on the state's email, or Internet systems.
3. No party may email PI unless using approved methods.
4. All emails between parties that contain or transmit PI must be encrypted before transmission.

C. Internal Security Controls with Communications to CVSOs/TVSOs:

1. **Release of Veteran-Claimant Information.** In alignment with USDVA procedures, the WDVA Bureau of Claims shall only release PI to those CVSO/TVSO and CVSO/TVSO staff who are officially "accredited" for USDVA purposes. If a CVSO/TVSO office does not have an accredited representative, the WDVA Claims Officer shall not discuss or provide any information specific to a pending claim unless authorized by the claimant during that specific communication. If the claimant is present in the CVSO/TVSO office at the initiation of such contact, the WDVA Claims Officer can speak directly to the claimant (after proper verification of identity using established USDVA protocol) to gain such authorization.
2. **Fax Messages.** The parties shall accept fax messages; however, neither party shall fax PI to unauthorized third parties without the written consent of the Veteran or the Veteran's duly appointed representative.
3. **Encrypted Messages Other than VA.** Parties to this Agreement when communicating with the WDVA Claims office must register for an email account through VA.Gov and utilize VA.Gov access and Personal Identification Verification Cards (PIV Cards) to ensure data security to accomplish any communication of PI with the WDVA Claims Office.
4. **Release of Veteran-PI by WDVA.** The WDVA Divisions of Veteran Benefits, Services and Homes, shall only release information by U.S. Mail, telephone or encrypted emails and when done consistent with applicable laws and policies.

IV. Non-Assignable. This Agreement shall be non-assignable.

V. Governing Law. This Agreement and all questions relating to its validity, interpretation, performance and enforcement (including, without limitation, provisions concerning limitations of actions}, shall be governed by and construed in accordance with the laws of the state of Wisconsin.

VI. Binding Nature of Agreement and Term. This Agreement shalt be binding upon and inure to the benefit of the parties and their respective successors and assigns, with a term of five (5) years from the date of the last signature below. In the event of substantial changes in the applicable law(s), parties may amend this Agreement or enter into a new Agreement to ensure compliance. In the event of a WDVA transition to a replacement of the VBATS tracking system, this Agreement shall continue to be binding and in effect for the replacement system(s) until such time as a new Agreement or amendment hereto shall be drafted between the parties. Access User/Receiving Party represents that he or she has authority to bind the County or Tribal Authority to this Agreement, and that the Executive head of the County or Tribal entity of the Access User/Receiving Party has approved this Agreement for execution.

VII. Umbrella Provision. This Agreement constitutes an umbrella agreement to the recipient's office, so long as any person accessing data who is accredited by the United States Department of Veterans Affairs, possesses a PIV Card, and is authorized by the Access User/Receiving Party to do so.

VIII. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties hereto and nothing herein, express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit or remedy of any nature whatsoever, under or by reason of this Agreement.

IX. Entire Agreement. This Agreement sets forth all of the covenants, promises, Agreements, conditions and understandings between the parties and there are no covenants, promises, Agreements or conditions, either oral or written, between them other than herein set forth. No subsequent alteration, amendment, change or addition to this Agreement shall be binding upon either party unless reduced in writing and signed by them.