Privacy Impact Assessment for the VA IT System called:

General Support System (GSS)

Date PIA completed:

August 14, 2014

VA System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Julie A. Lowery</td>
<td><a href="mailto:julie.lowery2@va.gov">julie.lowery2@va.gov</a></td>
<td>(269) 966-5600, ext. 31603</td>
</tr>
<tr>
<td>Information Security Officer</td>
<td>Deven Cook</td>
<td><a href="mailto:deven.cook@va.gov">deven.cook@va.gov</a></td>
<td>(269) 223-3956</td>
</tr>
<tr>
<td>System Owner</td>
<td>John Caras</td>
<td><a href="mailto:john.caras@va.gov">john.caras@va.gov</a></td>
<td>(269) 966-5600, ext. 36215</td>
</tr>
<tr>
<td>Person Completing the Document</td>
<td>Julie A. Lowery</td>
<td><a href="mailto:julie.lowery2@va.gov">julie.lowery2@va.gov</a></td>
<td>(269) 966-5600, ext. 31603</td>
</tr>
</tbody>
</table>
Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system.
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- A citation of the legal authority to operate the IT system.

The owner of the General Support System (GSS) is the Battle Creek VA Medical Center (VAMC), Station 515. The GSS is comprised of workstations, servers, printers and other equipment which include devices such as routers, hubs, switches, and firewalls that support communications to extended LAN locations such as community based outpatient clinics (CBOC’s). The GSS also includes subsystem components such as tape drives, disk drives, uninterruptible power supplies (UPS), network area storage (NAS), and storage access networks (SAN). Within this plan each facility will document their own physical description of their LAN system including local and extended LAN locations, its components and subsystems. Access to the LAN system is via wired or wireless devices using TCP/IP and other protocols operating on a variety of operating systems including UNIX, Linux, and Windows-family operating systems. Devices which access the LAN system include government furnished equipment (GFE) such as: personal computers, thin clients, various models of “dumb” terminals, portable computing devices and medical device systems. Clients primarily connect over the TCP/IP network using terminal emulation software and remote procedure call (RPC) broker to VistA or other network resources such as file, print or application servers and telephone systems. Access to external resources outside the LAN boundary will conform to national wide area network (WAN) guidelines on configuration and usage. WAN security is outside facility control and beyond the scope of this document. The Battle Creek VAMC LAN system is connected to the Internet. System level controls included NTFS file security protection in which access is limited to authorized groups of users.

The expected number of individuals, whose information is stored in the system, is 100,000 plus. The typical client or individuals, which have Personally Identifiable Information (PII) or Protected Health Information (PHI) stored on the GSS are Veterans, employees, volunteers, Compensation Work Therapy (CWT) workers, students, and Without Compensation workers (WOC).

The information collected, stored, and used on the GSS includes medical records (health records), employee health records, personnel records, volunteer records, work therapy records, claims/billing records, eligibility records, humanitarian/collateral records, and research records.

The legal authority to operate this system are 38 U.S.C. 501(b) and 304.
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see the VA Handbook 6500 (http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=638&FType=2, published Sept. 2012, Appendix A.)

If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- Email Address
- Emergency Contact Information (Name, Phone)
- Number, etc of a different individual
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity

Current medical records, language needs, criminal record information, service information, guardian information, education information, benefit information, claim/billing information, audit reports, safety and quality reports.

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?
The information is collected by the individual, state websites (police-lien, prescription drug monitoring), eligibility forms, Veterans Benefits Administration (VBA), Health Eligibility Center (HEC), providers, and Department of Defense (DOD).

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The sources of information are from the individual, individual’s guardian or Power of Attorney (POA), individual’s family member, providers of care [both (Veterans Administration) VA and non-VA Care], state websites (police-lien, prescription drug monitoring), eligibility forms, VBA, HEC, DOD, employee input of information, applications for benefits, research, diagnostic testing, and data input from internal sources.

Information from other sources than the individual would be for incompetency of the individual, either court ordered or invoked due to provider authentication. Other information from support staff and providers would be entered into the system to provide health care to the individual, bill for health care, determine eligibility for the individual. Personnel information may be entered by the Human Resources Management office for performance evaluation, workmen compensation, and contractors.

The police use the state Law Enforcement Information Network (LEIN) website to acquire arrest information. Providers receive information from other providers for continuity of care. The VBA and HEC provide information on enrollment and eligibility. The State Drug Monitoring Program allows providers to view controlled substances that have been provided. The state immunization website allows providers to acquire immunization records. DOD records can be shared for continuity and coordinating care for new Veterans.

The information can run reports for quality measures, audit purposes, scheduling, patient care, and eligibility requirements.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

The information is collected from the individual, other legal representative, VA Form DD 214, VA Form 10-10 (EZ, EC, HS CG), VA Form 0750, employee supervisors, providers, research activities, and contractors. Criminal record information and state drug prescription monitoring (MAPS) are accessed through the website using state portals. The website is used to connect to the HEC and VBA databases for benefit and eligibility information. Information can be transmitted via encrypted email and facsimile (fax). Claims information is retrieved electronically. Various forms are used locally to collect information, which is transferred into CPRS and the form shredded. Various VA Forms are used, as follows: VA Form 10-2364 for Audiology Reports, SF 518 for Blood Transfusions, VA Forms 10-5345 & 10-5345a for Release of Information, VA Form 10-
1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publically available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This information is collected for Veteran healthcare, claims, eligibility, law enforcement activity, personnel/human resources, administrative, and benefits processing. Commercial data is released through FOIA processing to show the transparency of the government agency. Employee information is collected to determine employment ratings, placement, and daily functions. In response to court orders information can be released.

1.5 How will the information be checked for accuracy?

Discuss whether and how information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency?

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Data is matched against supporting documentation submitted by the Veteran. Social Security Numbers are verified through the Social Security Administration (SSA) to determine financial eligibility. The VBA is used to verify eligibility for VA benefits. The VA verifies military service information through the DOD. Financial information is verified through the SSA and Internal Revenue Service (IRS).

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

The legal authority that allows for the collection of Social Security Number is Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for
individual's rights, benefits, and privileges under federal programs. The system is permitted under Routine Use under legal authorities for the System of Records, as follows:

- Title 38, United States Code (U.S.C.), Sections 501(b) and 304 for medical records;
- 40 Federal Register (FR) 38095 & 66 FR 20860 for Blood Donor Information and Ionizing Radiation Registry-VA;
- 67 FR 61205, Privacy Act of 1974, 5 U.S.C. 552a(e) for Non-VA Fee Basis Records;
- 58 FR 40852 Veteran, Employee, and Citizen Health Care Facility Investigation Records-VA;
- 40 FR 38095 & 59 FR 16705 Veteran, Employee and Volunteer Research and Development Project Records-VA;
- 38 U.S.C., Sections 501(a), 501(b), 1703, 1724, 1725, 1728, 1802, 1803, 1813, and Public Law 103-446, Section 107 Health Administration Center Civilian Health and Medical Program Records-VA; 38 U.S.C, Section 513 Voluntary Service Records-VA;
- 38 U.S.C., Section 1712a Readjustment Counseling Service-VA; 38 U.S.C., Sections 210(c), 610, and 4101 Community Placement Program-VA;
- 38 U.S.C., Sections 501(a), 1705, 1710, 1722, & 5317 Income Verification Records-VA;
- 38 U.S.C., Section 501 Call Detail Records-VA;
- 38 U.S.C., Chapter 73, Section 7301(b) Patient Advocate Tracking System (PATS)-VA;
- 38 U.S.C., Section 501 Compliance Records, Responses and Resolutions of Reports of Persons Allegedly Involved in Compliance Violations-VA;
- 38 U.S.C., Sections 501, 503, 7451, 7452, & 7431-7440 Employee Incentive Scholarship Program-VA;
- 38 U.S.C., Section 501 Telephone Care and Service for Clinical Care;
- 38 U.S.C., Sections 1710 & 1729 The Revenue Program-Billing and Collections Records-VA;
- 38 U.S.C., Sections 501, 503, 7451, 7452, and 7431-7440 Education Debt Reduction Program-VA;
- 38 U.S.C., Part V, Chapter 78 Veterans Canteen Service (VCS) Payroll Deduction Program (PDP)-VA; 38 U.S.C., Section 501 National Patient Databases-VA;
- 38 U.S.C., Section 501 My HealtheVet Administrative Records-VA;
- 73 FR 55214 Library Network (VALNET)-VA;
- 38 U.S.C., Section 1730 Residential Care and Medical Foster Home Programs-VA;
- 38 U.S.C., Sections 501(a), 1705, 1710, 1722, and 5317 Enrollment and Eligibility Records-VA;
- 38 U.S.C., Sections 501 & 7304 Administrative Data Repository-VA;
- 38 U.S.C., Sections 501(b), 304, 7301, & 7304(a) Ethics Consultation Web-based Database (ECWeb)-VA; 38 U.S.C., Sections 501(a), 1705, 1710, 1722, 1722(a), 1781 and 5 U.S.C., Section 552(a) Customer Relationship Management System (CRMS)-VA;
1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

**Principle of Purpose Specification:** Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

**Principle of Minimization:** Is the information directly relevant and necessary to accomplish the specific purposes of the program?

**Principle of Individual Participation:** Does the program, to the extent possible and practical, collect information directly from the individual?

**Principle of Data Quality and Integrity:** Are there policies and procedures for DHS to ensure that personally identifiable information is accurate, complete, and current?

Follow the format below when entering your risk assessment:

**Privacy Risk:** The information that is collected at the Battle Creek VAMC contains both Personally Identifiable Information (PII) and Protected Health Information (PHI). Due to the sensitive information of names, addresses, date of birth, SSN, dependents and health information, the potential of a breach could exist. If this information was breached or compromised, it could have a high risk of harm to the individual’s professional, personal, and financial aspects of life.

**Mitigation:** Mitigations to protect Privacy include technical, physical, and administration controls. The users of the information are provided Privacy, HIPAA, and Rules of Behavior on an annual basis. The facility has a Chief Information Officer, Information Security Officer, and Privacy Officer on staff to assist and monitor in protecting the individual’s information. Users of the information are only given access to electronic and paper documents that are needed to complete their duty tasks.

Section 2. Uses of the Information
The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program’s business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.

The information is collected or maintained, both internally and externally, for the purpose of healthcare treatment, payment, and healthcare operations.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system can make or create new or previously utilized information about an individual. The information is documented in the Computerized Patient Record System (CPRS). This information will be used by administrative, healthcare support staff, and healthcare professionals for healthcare treatment, payment, and healthcare operations. The information systems undergo maintenance schedules, monitors, and audits.

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-53 and specific VA directives.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.
Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

Controls in place to ensure that information is handled in accordance with the uses described above include annual Privacy, HIPAA, and Rules of Behavior training for all employees and contractors; privacy and security briefing during new employee orientation, and ongoing educational training by the Privacy Officer and Information Security Officer. Users of the information are only given controls to access the information that is essential and pertinent to complete their duty assignments. The PIA and SORN are clear about the uses of information under “routine use”. The information contained in the system is relevant to the mission of the VHA for treatment, payment, and healthcare operations. Any violations of access or use of the information are investigated by the Privacy Officer and Information Security Officer and referred to the supervisor and human resources for disciplinary action.

### Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

#### 3.1 What information is retained?

All information collected, stored, and used is for healthcare and historical information follows the Record Control Schedule (RCS) 10-1 for VHA and (RCS) 005-1 for Office of Information and Technology retention guidelines, except for temporary files. Temporary files, also known as working papers, are documents used that to make the electronic entries of information or used to temporarily and destroyed when no longer needed by the user.

#### 3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*

Medical records are retained for 75 years after the last date of activity. Personnel, administrative, and business records are retained for various amounts of time. The guidance for retention of records is found in the RCS 10-1, RCS VB-1, Part II Revised for VBA, and the National Archives and Records Administration.
3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

The retention has been approved by the National Archives and Records Administration (NARA). The guidance for retention of records is found in the RCS 10-1, RCS VB-1, Part II Revised for VBA, and the National Archives and Records Administration.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

Paper records and Compact Discs (CDs) on site are shredded by a contractor with Certificates of Destruction obtained, per NIST standards. Electronic destruction has not yet been determined.

3.5 **PRIVACY IMPACT ASSESSMENT: Retention of information**

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

Follow the format below:

**Privacy Risk:** High-the information retained could be subject to breach, loss, or unintentional destruction from external, internal, and physical risks.

**Mitigation:** The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed. The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy. A process of centralized storage for the facility is being reviewed.
Section 4. Internal Sharing and Disclosure

The following questions are intended to define the scope of information sharing within VA.

4.1 With which internal organizations is information shared? What information is shared, and for what purpose? How is the information transmitted or disclosed?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific information is shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

<table>
<thead>
<tr>
<th>Program Office or IT System information is shared with</th>
<th>Reason why information is shared with the specified program or IT system</th>
<th>List the specific information types that are shared with the Program or IT system</th>
<th>Method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUSE-CPRS Veterans Benefits Administration (VBA)</td>
<td>Veterans’ benefits and eligibility</td>
<td>PHI/PII</td>
<td>LAN</td>
</tr>
<tr>
<td>Dictation-PowerScribe</td>
<td>Transcription of encounters</td>
<td>PHI/PII</td>
<td>LAN</td>
</tr>
<tr>
<td>Citrix</td>
<td>Health Information and remote access of desktops</td>
<td>PHI/PII</td>
<td>LAN-Remote Server</td>
</tr>
<tr>
<td>Electronic Payroll Deduction/Electronic Card System</td>
<td>Deduction for purchases through payroll</td>
<td>PII</td>
<td>LAN</td>
</tr>
<tr>
<td>ScriptPro</td>
<td>Pharmacy Reporting</td>
<td>PHI/PII</td>
<td>LAN</td>
</tr>
<tr>
<td>HP/TRIM (CIRTS) CBI</td>
<td>Business Compliance Activities, causation, and corrective action</td>
<td>Business Information</td>
<td>LAN</td>
</tr>
<tr>
<td>CPRS, Health Eligibility Center (HEC)</td>
<td>Eligibility of Veteran services</td>
<td>PHI/PII</td>
<td>LAN</td>
</tr>
<tr>
<td>System/Software</td>
<td>Function/Information Provided</td>
<td>PHI/PII</td>
<td>Type of Storage</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>McKesson</td>
<td>Pharmacy Purchasing</td>
<td>Procurement Information</td>
<td>LAN</td>
</tr>
<tr>
<td>NOAH</td>
<td>Audiology Testing</td>
<td>PHI/PII</td>
<td>CPRS</td>
</tr>
<tr>
<td>Auditory Brainstem Response (ABR)</td>
<td>Audiology Testing</td>
<td>PHI/PII</td>
<td>CPRS</td>
</tr>
<tr>
<td>Otoacoustic Emissions Testing</td>
<td>Audiology Testing</td>
<td>PHI/PII</td>
<td>CPRS</td>
</tr>
<tr>
<td>IMH-Psychiatry</td>
<td>Logs, staff telephone numbers, meeting minutes, guidelines, personal lists</td>
<td>PII</td>
<td>Computer</td>
</tr>
<tr>
<td>VetPro/PrivPlus</td>
<td>Credentialing-privileging</td>
<td>PHI/PII</td>
<td>Computer/FAX</td>
</tr>
<tr>
<td>VSSC Data Warehouse</td>
<td>Medical Foster Home/Teleretinal</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Mobile Electronic Documentation</td>
<td>Medical Foster Home/Teleretinal</td>
<td>PHI/PII</td>
<td>Mobile devices-VPN</td>
</tr>
<tr>
<td>ASR, CWS, Electronic Card System (ECD),</td>
<td>Electronic Payroll Deduction, Purchase Payment Agreements, Cash Receipts, Journals and Credit Card Transactions</td>
<td>PII/Financial Information</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>ASR, CWS, Electronic Card System (ECD),</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Payroll Deduction (EPD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web HR, eQip, PIV, TMS Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance, eOPF, Position Descriptions, P&amp;R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computation Calculator, USA Staffing, ECF,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occupational Health Record System (OHRS), Workers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compensation (WC), Occupational Safety &amp; Health</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management System (OSHMIS), Employee Compensation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations &amp; Management Portal (ECOMP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AEMS/MERS</td>
<td>Equipment maintenance and repair Safety Compliance</td>
<td>PHI/PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>BrainTrain IVA Plus Test, KayPentax Videostrobe,</td>
<td>Veteran Healthcare for speech</td>
<td>PHI/PII</td>
<td>Computer/LAN</td>
</tr>
<tr>
<td>DICOM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fee Basis Claims System (FBCS)</td>
<td>Non VA Care Claims</td>
<td>PHI/PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>Application/Part of System</td>
<td>Function/Use Case</td>
<td>PHI/PII</td>
<td>Computer/LAN</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>DSS ROI</td>
<td>Release of information accounting of disclosure tracking</td>
<td>PHI/PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>FOIAxpress</td>
<td>Freedom of Information Act request tracking system</td>
<td>Request information-PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>BMC Remedy-Privacy &amp; Security Event Tracking System (PSETS)</td>
<td>Privacy and security incidents and complaints tracking</td>
<td>Tracking System</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>Adobe Acrobat</td>
<td>Scanning documents, creating PDF files.</td>
<td>PHI/PII, business information</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>AUTOCAD</td>
<td>Engineering/designing</td>
<td>Blueprints</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>CareTracker</td>
<td>Veteran’s healthcare</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>CHECKPOINT</td>
<td>Monitors temperature on refrigerators throughout the Healthcare Delivery system</td>
<td>Health and safety</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>General Med. Rec.-Generator</td>
<td>Transfers vitals into CPRS for Veteran healthcare</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>GMED</td>
<td>Global media for teleconferencing transmits to provider for vitals</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Sentillion</td>
<td>VPN access for healthcare</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Stentor</td>
<td>Allows providers to see radiology images in the PACS for treatment of Veterans</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>TopCon</td>
<td>Teleretinal imaging</td>
<td>PHI/PII</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Lynx Duress Alarm</td>
<td>Emergency Alarm</td>
<td>Building and room number</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Microsoft Office Lync</td>
<td>Instant messaging</td>
<td>PHI/PII use, not storage</td>
<td>Computers-LAN</td>
</tr>
<tr>
<td>Missing Patient Reg (Original) A4EL</td>
<td>Missing patient information</td>
<td>PHI/PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>Police and Security</td>
<td>Law enforcement activities</td>
<td>PII</td>
<td>Computer-LAN</td>
</tr>
<tr>
<td>Secure messaging</td>
<td>My HealtheVet messaging</td>
<td>PHI/PII</td>
<td>Computer-CPRS</td>
</tr>
<tr>
<td>DICTATON-PowerScribe</td>
<td>Transcription</td>
<td>PHI/PII</td>
<td>Telephone, Computer, LAN</td>
</tr>
<tr>
<td>Drug Accountability</td>
<td>Pharmacy</td>
<td>PHI/PII</td>
<td>Computer-LAN</td>
</tr>
</tbody>
</table>
### MUSE

<table>
<thead>
<tr>
<th>EKGs</th>
<th>PHI/PII</th>
<th>Computer-LAN</th>
</tr>
</thead>
</table>

### PACS Database

<table>
<thead>
<tr>
<th>Radiology Images</th>
<th>PHI/PII</th>
<th>Computer-LAN</th>
</tr>
</thead>
</table>

### Computerized Patient Record System (CPRS)

<table>
<thead>
<tr>
<th>Veteran’s health and eligibility information</th>
<th>PHI/PII</th>
<th>Computer-LAN</th>
</tr>
</thead>
</table>

### Office of Inspector General

<table>
<thead>
<tr>
<th>Healthcare oversight &amp; law enforcement</th>
<th>PHI/PII</th>
<th>Computer, Fax, encrypted email, and in person</th>
</tr>
</thead>
</table>

### Local SharePoints

<table>
<thead>
<tr>
<th>Business, work flow processes, healthcare operations</th>
<th>PHI/PII (secured)</th>
<th>Computer</th>
</tr>
</thead>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Follow the format below:

**Privacy Risk:** High, as potential loss could occur due to theft or destruction.

**Mitigation:** Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy, security, and records management.

### Section 5. External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

#### 5.1 With which external organizations is information shared? What information is shared, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific information is shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?
Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

<table>
<thead>
<tr>
<th><strong>Program Office or IT System</strong></th>
<th><strong>Reason why information is shared with the specified program or IT system</strong></th>
<th><strong>List the specific information types that are shared with the Program or IT system</strong></th>
<th><strong>Legal authority, binding agreement, SORN routine use, etc that permit external sharing (can be more than one)</strong></th>
<th><strong>Method of transmission and measures in place to secure data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Providers</td>
<td>State reporting of epilepsy</td>
<td>PHI/PII</td>
<td>With written request for mandated state reporting</td>
<td>Data portal</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>VHA staff-release of information, Administrative Officer of the Day</td>
<td>Coroner/medical examiner</td>
<td>PHI/PII-no U.S.C. 7332</td>
<td>Routine Use 24VA10P2</td>
<td>Telephone, fax</td>
</tr>
<tr>
<td>Providers, social work, release of information, nursing, clerks</td>
<td>External providers, healthcare facilities, nursing homes, adult foster care homes for coordinating and continuity of care.</td>
<td>PHI/PII-no U.S.C. 7332</td>
<td>Routine Use 24VA10P2 and 142VA114, MOUs</td>
<td>Telephone, fax</td>
</tr>
<tr>
<td>Laboratory</td>
<td>Food &amp; Drug Administration for healthcare oversight</td>
<td>PHI/PII</td>
<td>Healthcare oversight and Routine Use 24VA10P2, 04VA115</td>
<td>Telephone, fax</td>
</tr>
<tr>
<td>Non VA Care</td>
<td>Third party insurance for payment</td>
<td>PHI/PII-no U.S.C. 7332</td>
<td>Payment-Routine Use-24VA10P2 &amp; 23VA16</td>
<td>Telephone, fax</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Access controls, audit and accountability, awareness and training, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, media protection, personnel security, physical and environmental protection, risk assessments, system and services
acquisition, system and communication protection, system and information integrity, planning, and maintenance are used to meet the requirements of OMB Memoranda M-06-15 and M-06-16.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments. Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

Follow the format below:

Privacy Risk: There is a risk that the information could be shared with an external organization or agency that does not have a legal authority to access VA data. The information could be re-disclosed by the external organization or agency.

Mitigation:
MOUs are reviewed by Regional Counsel and the Privacy Officer prior to issuing. The DUAs are reviewed by the Information Security Officer, Privacy Officer, and Regional Counsel. Standing letters are valid for three (3) years, at which time, a letter is sent to request renewal from the head of the agency for the standing letter. Standing letters are monitored by the Privacy Officer and service. DUAs and MOUs are monitored by the service area chief.

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Section 6. Notice
The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The Notice of Privacy Practices, updated September 23, 2013, is mailed to the Veteran at the time of enrollment. If there are updates to the Notice of Privacy Practices, they are bulk mailed to all enrolled Veterans. Any non-Veteran requiring treatment will receive a Notice of Privacy Practices at the time of treatment. There are Notice of Privacy Practices in the facility in various locations and at all the Community Based Outpatient Clinics (CBOCs). The Notice of Privacy Practices can be found on the VA Privacy Service webpage (http://www.privacy.va.gov/Privacy_Resources.asp), eHealth webpage (http://www.ehealth.va.gov/VA_DOD_Health_Partnership.asp), and at www.va.gov/vaforms. A person could you a search engine to find the Notice of Privacy Practices.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

The person has a right to decline to provide information; however, the VHA may not be able to enroll the Veteran. The Notice of Privacy Practices states that the Veteran has the right to request a restriction of the use and disclosure of information; however, under 45 CFR § 164.522(a)(1)(vi) the VHA is not required to agree to such a restriction.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

The Veteran has the right to consent to use of U.S.C. 7332 (Alcohol and Substance Abuse, HIV, and Sickle Cell Anemia) and medical records by completing the VA Form 10-5345 to authorized third parties information. Treatment, payment, and healthcare operations will require Veteran authorization for the use of U.S.C. 7332 information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:
**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

Follow the format below:

**Privacy Risk:** There is a risk that Veterans, employees, or general public may not be aware of the collection, maintenance, and dissemination of PII/PHI about them through the existence of the Battle Creek VAMC GSS.

**Mitigation:** The risk of the Veteran not receiving “Notice” is low; however, the risk of information being used for another purpose other than what is articulated in the notice is moderate to high, as individuals could mistakenly use information inappropriately. Access controls, physical controls, technical controls, audits/monitors, and ongoing education of information use is active to mitigate risk of information used inappropriately.

**Section 7. Access, Redress, and Correction**

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

**7.1 What are the procedures that allow individuals to gain access to their information?**

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

Individuals follow procedures to gain access to their information under the guidelines of the Privacy Act, Freedom of Information Act (FOIA), and Health Insurance Portability and Accountability Act (HIPAA).

**7.2 What are the procedures for correcting inaccurate or erroneous information?**

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

The Veteran should provide a written request, with signature, for correcting of inaccurate or erroneous information to the Privacy Officer of the Battle Creek VA Medical Center by writing to: Privacy Officer
If corrections are needed for legal name, date of birth, or Social Security Number (SSN) changes, the Privacy Officer would process the request requiring a valid driver’s license, state identification, passport, military ID, or a letter from the Social Security Administration stating the changes and a wet signature from the individual requesting the change.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

The Notice of Privacy Practices explains the Veteran’s right to request a correction to inaccurate, erroneous, untimely, or incomplete information. The facility and CBOC staff and providers are educated to refer the Veteran to the Privacy Officer for requests to correct their records. At the time of the request the individual is sent an acknowledgement letter and they are sent a letter at the completion of processing regarding the outcome of the requested correction.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Redress is provided through the Privacy Act for the individual to view and request correction to the inaccurate or erroneous information. If the request is denied, the individual to appeal the decision by writing to the Office of General Counsel (024); Department of Veterans Affairs; 810 Vermont Avenue, N.W.; Washington, D.C. 20420.

The Privacy Act and HIPAA permit the individual to also complete a Statement of Disagreement to the information that was denied correction. The facility would be able to include a rebuttal to the Statement of Disagreement. The Statement of Disagreement, rebuttal, and denial letter would be attached to the information that was requested to be corrected and would be released with the information at any time the information was authorized for release.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if
a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Follow the format below:

Privacy Risk: There is a risk of an individual not receiving notifications pertaining to appointments, medications, test results, and benefit information when the record contains incorrect information. Incorrect information documented in a record could result in improper healthcare diagnosis and treatment.

Mitigation: The Privacy Risk is low-moderate, as the information is processed through the Privacy Act, HIPAA, and FOIA. FOIA protects specific records with exemptions. When information is processed under FOIA, the exemptions and an explanation of the exemption are included in the response to the request. The individual has a right to access of their individual information under the Privacy Act, when that information is part of a Privacy Act System of Records. An individual’s identity is confirmed in requesting access, redress, and correction of information through legal authority (POA, Guardian, Next of Kin), photo identification and/or wet signature, which protect the information from being used without the individual’s knowledge. Appeal rights are given to an individual upon denial of a correction.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system.

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
An individual is assigned menu options and keys delegated by the type of access they need to complete their duty tasks. The supervisor maintains a functional category form on employees that is reviewed annually to ensure proper menu options and keys are delegated for the employee to complete duty tasks. Keys and menu options are not given if not required by the employee’s duty task. Monitors and audits are completed on the functional categories by the Privacy Officer and Information Security Officer.

8.2 Will VA contractors have access to the system?

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required.*

VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete their duty task. They are required to complete annual Privacy, Security, and Rules of Behavior training. Contractors having access to PHI/PII are required to complete a Business Associate Agreement. Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Security, and Rules of Behavior training is completed by contractors and business associates.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. *Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.*

Contractors are required to take annual Privacy, Security, and Rules of Behavior Training through the Talent Management System (TMS) course 10176 and 10203 or through completing GAP Training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

*If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.*

There is not an ATO for GSS. There is a Temporary Authority to Operate, which was signed August 1, 2014.
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

________________________________________
Privacy Officer, Julie A. Lowery

________________________________________
Information Security Officer, Deven Cook

________________________________________
System Owner, John Caras

________________________________________
Individual Completing the PIA, Julie A. Lowery