Privacy Impact Assessment for the VA IT System called:

IOW-VHA VistA

Iowa City VA Health Care System

Date PIA completed:

November 21, 2017

VA System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Makenzie Johnson</td>
<td><a href="mailto:Makenzie.Johnson@va.gov">Makenzie.Johnson@va.gov</a></td>
<td>(319) 338-0581, 6092</td>
</tr>
<tr>
<td>Information Security Officer</td>
<td>Randall E. Smith</td>
<td><a href="mailto:Randall.Smith@va.gov">Randall.Smith@va.gov</a></td>
<td>(319) 338-0581, 6266</td>
</tr>
<tr>
<td>Information Security Officer</td>
<td>Robert Hensley</td>
<td><a href="mailto:Robert.Hensley3@va.gov">Robert.Hensley3@va.gov</a></td>
<td>(319) 338-0581, 6265</td>
</tr>
<tr>
<td>System Owner</td>
<td>Stan Bush, Director Operations, Midwest T1 for Robert L. Page, III Director, Continental District</td>
<td><a href="mailto:Stan.Bush@va.gov">Stan.Bush@va.gov</a></td>
<td>(651) 405-5680</td>
</tr>
<tr>
<td>Person Completing the Document</td>
<td>Makenzie Johnson</td>
<td><a href="mailto:Makenzie.Johnson@va.gov">Makenzie.Johnson@va.gov</a></td>
<td>(319) 338-0581, 6092</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

Veterans’ Health Information Systems and Technology Architecture (VistA) is a highly integrated system which runs administrative and clinical applications. Each Veterans Affairs (VA) medical center uses VistA an integrated hospital information system. VistA is structured so that it can be customized in certain specialized areas and most local medical centers have taken advantage of this flexibility. Applications within VistA support a multitude of areas including medical imaging, supply management, decision support, medical research, and education.

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. Additionally, what region is the system under?
- 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 Iowa City VA Health Care System’s VistA System, officially known as IOW-VHA-VistA is a facility level entity that operates under the authority of Veterans’ Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a). The VistA (e.g., All facility VistA systems will be rolled up into one Regional VistA boundary consisting of VistA MUMPS environment (Massachusetts General Hospital Utility Multi-Programming System, later changed to Multi-User Multi-Programming System and now referred to as "M" programming language); its applications, users stored in “dat” files) to support mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration by providing access to electronic resources.

Iowa City VA Health Care System collects, processes, and/or retains the information of over 184,000 Veterans, 2,774 students, contractors and VA employee information.

The Region 2 VistA boundary was newly created in 2013 when the Office of Information and Technology made major changes to VA systems and their security boundaries. Although the Regional 2 VistA information system boundary does provide security oversight and a variety of support functions to the facilities and their local VistA Systems, data ownership remains at the facility level and many of the decisions related to the collection, use, storage, and dissemination of the data are made at the facility level.
The Iowa City VA Health Care System VistA system (Omaha integrated database) was relocated to the St. Louis, Missouri Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) on October 18, 2014.

The Iowa City VA Health Care System staff independently decides whether or not to share data with other sources as stated throughout this document. The ICVAHCS conducts a variety of information sharing internal and external to the Department of Veterans Affairs. Internal sharing is discussing in greater detail in Section 4 of this Privacy Impact Assessment (PIA). This type of sharing is done to ensure that veterans and their families receive the necessary care and benefits. External sharing, which is discussed in greater detail in Section 5 of this PIA is done with other agencies and organizations.

The legal authorities to operate the VistA system are Title 5, United States Code, section 301, Title 38, United States Codes, sections 109, 111, 501, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, and 7105 and Title 38, United States Code, Section 7301 (a).

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
• Gender as provided by the patient
• Name and contact information for Guardian as provided by the patient
• Military and service history as provided by the patient and/or VBA
• Employment information as provided by the patient
• Veteran dependent information as provided by the patient
• Education information as provided by the patient
• Medical statistics for research purposes containing PII/PHI
• Name and contact information for Next of Kin
• Service Connected rating and disabilities (based on information provided by Veteran and/or VBA)
• Date of death as supplied by Next of Kin or provider
• Criminal background and dependent information as reported by patient and/or national databases
• Medical record
• Contractor and employee personnel and payroll records

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?

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.

As the Region 2 VistA contains a large amount of data on a wide variety of individuals, the sources of data are varied.

The information collected, maintained and/or disseminated by ICVAHCS comes from a variety of resources. The largest amount of data comes directly from individuals - including veterans and their dependents, volunteers and other members of the public, clinical trainees, and VA employees and contractors.

Iowa City VA Health Care System also collects data already provided to other organizations within the VA, including:
• Veteran’s Benefit Administration (VBA)
• Austin Automation Center (AAC)
• Health Eligibility Center (HEC)
• National Cemetery Administrations (NCA)
• VA Veteran Centers
• Department of Veterans Affairs General Counsel Office
• Consolidated Patient Accounts Center (CPAC)

For VBA we collect data for eligibility information and benefits; Austin Automation Center data is collected for financial records; Health Eligibility Center data is collected for eligibility information on Veterans; National Cemetery Administration to send verification of death and benefit records; VA Veterans Centers to treat Veterans/eligibility; Department of Veterans Affairs General Counsel Office to process and assist with legal issues and guidance; and CPAC to collect data for billing purposes. Iowa Department of Health to provide information related to public health concerns of Veterans as required by Iowa state law.
Additional data, such as confirmation of military service or results of employee background checks, come from external Federal Agencies. These agencies include:

- Department of Defense (DOD)
- Internal Revenue Service (IRS)
- Office of Personnel Management (OPM)
- Social Security Administration (SSA)
- Federal Emergency Management Agency (FEMA)
- Federal Bureau of Investigation (FBI)

We collect data for background checks and security clearances for all the agencies listed above as well as confirmation of military services. FEMA to communicate in emergency situations; IRS to communicate Veterans financial information; SSA for social security benefits; and OPM to communicate employee information for employment purposes.

- State Prescription Drug Monitoring Program

We communicate medication information with the State Prescription Drug Monitoring Program to meet state requirements for prescribing narcotics.

### 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.

Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, Request For and Authorization To Release Medical Records Fillable), and via electronic and web form submissions.

Information is also collected from a variety of other IT systems and resources (which is mentioned in Section 4 and 5) internal and external to the VA. These data collections may be done using secure web portals, VPN connection, e-mail and facsimile.

### 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.

Much of the information collected is maintained, used, and disseminated by ICVAHCS to ensure that Veterans and other eligible individuals obtain the medical and mental health treatment they require. Additional information, such as bank account information and insurance information are used to process claims and requests for benefits.
Other purposes include determination of legal authority for providers and other clinical staff to practice medicine and/or subject matter expertise, release of information request responses, and research/analysis of data.

Employee and VA contractor information is maintained based on Human Resources (HR) and payroll needs and Federal contracting requirements.

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.

Information obtained directly from the individual will be assumed to be accurate. Information may be verified with other Federal agencies (VBA, DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information come to the attention of facility staff, it will be documented and verified prior to further use.

Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center are obtained. Practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections.

Employee, contractor, student and volunteer information is obtained by automated tools as well as obtained directly by the individuals. The Federal Bureau of Investigation and Office of Personnel Management are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources.

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 Iowa City VA Health Care System VistA System officially known as IOW-VHAVistA is a facility level entity that operates under the authority of Veterans’ Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Privacy Act of 1974
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 IOW-VHA VistA contains sensitive personal information – including social security numbers, names, dates of birth and protected health information – on veterans, members of the public, & VA employees and contractors. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation:

Veterans Health Administration (VHA), Region 2 as well as Iowa City VA Health Care System deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. Region 2’s security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.
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.

Due to the extensive amount and nature of the information contained in the Iowa City VA Health Care System VistA system, within the Region 2 VistA information system boundary, it is impossible to independently list each data point collected and describe its purpose. Below is a description of how different categories of data are used. If you have questions about a certain data point, please contact your facility privacy officer to learn more.

- **Name:** Used to identify the patient during appointments and patients and employees in other forms of communication.
- **Social Security Number:** Used as a patient and employee identifier and as a resource for verifying income information with the Social Security Administration.
- **Date of Birth:** Used to identify age and confirm patient identity.
- **Mother’s Maiden Name:** Used to confirm patient identity.
- **Mailing Address:** Used for communication, billing purposes and calculate travel pay.
- **Zip Code:** Used for communication, billing purposes and calculate travel pay.
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct tele health appointments.
- **Fax Number:** Used to send forms of communication and records to business contacts, insurance companies and health care providers.
- **Email Address:** Used for communication and myHealthevet secure communications.
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual):** Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility.
- **Health Insurance Beneficiary Account Numbers:** Used to communicate and bill third party health care plans.
- **Certificate/License numbers:** Used to track and verify legal authority to practice medicine and licensure for health care workers in a particular area of expertise.
- **Vehicle License Plate Number:** Used to track vehicles on VA grounds by VA Police to quickly identify vehicle ownership and authorization to be on facility grounds.
- **Internet Protocol (IP) Address Numbers:** Used to track, identify and locate a device on a network and to ensure no two devices are assigned the same IP.
- **Gender:** Used for patient demographic information.
- **Previous Medical Records:** Used for continuity of health care.
- **Current Medications:** Used within the medical records for health care/treatment purposes.
- **Race/Ethnicity:** Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Next of Kin:** Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information:** Used when a representative has been appointed or designated because the patient is unable to make decisions.
- **Military history/service connection:** Used to evaluate medical conditions that could be related to location of military time served. Also used to determine VA benefit and health care eligibility.
• **Service connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs.
• **Employment information**: Used to determine VA employment eligibility and for Veteran contact, financial verification.
• **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
• **Education information**: Used to determine VA employment eligibility as well as for patient health care/treatment purposes.
• **Medical statistics**: Used for research purposes containing PII/PHI.
• **Date of Death**: Used for death certificate, benefits and memorial honors.
• **Criminal background**: Used to determine VA employment eligibility as well as patient health care/treatment purposes.

The data may be used for research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; the registration of vehicles and the assignment and utilization of parking spaces; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations.

### 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.

Patient and employee data is analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. The Iowa City VA Health Care System uses statistics and analysis to create various reports which provide a better understanding of patient care and employee needs.

These reports may track:
• The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc. for Veterans established with a Patient Care Aligned Team (PACT)
• Beneficiary travel summary/benefits
• Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
• Daily bed management activity
• Coding averages for outpatient/inpatient encounters
• Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
• Unique patient trends
Clinic wait times

A complete list of the nationally released VistA Class 1 software packages may be obtained at http://www.va.gov/vdl/.

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?

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

Prior to signing into VistA, system users are provided the below banner of Notice to User sign-on:

VA systems are intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized for official business and limited personal use under VA policy.

Information from this system resides on and transmits through computer systems and networks funded by the VA. All access or use constitutes understanding and acceptance that there is no reasonable expectation of privacy in the use of Government networks or systems. All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action including (but not limited to) monitoring recording copying auditing inspecting investigating restricting access blocking tracking disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel.

Unauthorized user attempts or acts to (1) access upload download change or delete information on this system (2) modify this system (3) deny access to this system (4) accrue resources for unauthorized use or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.

********************************************************************
** WARNING ** WARNING ** WARNING **
THIS U.S. GOVERNMENT COMPUTER SYSTEM IS FOR OFFICIAL USE ONLY. THE FILES ON THIS SYSTEM INCLUDE FEDERAL RECORDS THAT CONTAIN SENSITIVE INFORMATION. ALL ACTIVITIES ON THIS SYSTEM MAY BE MONITORED TO MEASURE NETWORK PERFORMANCE AND RESOURCE UTILIZATION; TO DETECT UNAUTHORIZED ACCESS TO OR MISUSE OF THE SYSTEM OR INDIVIDUAL FILES AND UTILITIES ON THE SYSTEM, INCLUDING PERSONAL USE; AND TO PROTECT THE OPERATIONAL INTEGRITY OF THE SYSTEM. FURTHER USE OF THIS SYSTEM CONSTITUTES YOUR CONSENT TO SUCH MONITORING. MISUSE OF, OR
Iowa City VA Health Care System staff is trained in specific VistA software based on job duties such as Computerized Patient Record System (CPRS), Scheduling, Billing, etc. Facilities – Training are specific to their privileges to include VistA imaging and iMed Consent. Dragon Naturally software training is a user based training module initiated by the end user once the software is installed by IT.

**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?

Identify and list all information collected from question 1.1 that is retained by the system.

Iowa City VA Health Care System follows national VA policies regarding information retention. The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

- 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
- Gender as provided by the patient
- Name and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Medical statistics for research purposes containing PII/PHI
- Name and contact information for Next of Kin
• Service Connected rating and disabilities (based on information provided by Veteran and/or VBA)
• Date of death as supplied by Next of Kin or provider
• Criminal background and dependent information as reported by patient and/or national databases

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.*

When managing and maintaining VA data and records, Iowa City VA Health Care System will follow the guidelines established in VA Record Control Schedule (RCS)-10 (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf) as well as RCS 005-1 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf).

These documents specify how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level.

For greater details related to records retention at the Veterans’ Health Administration, please review RCS-10 and RCS-005-1.

Below are some key record retention schedules for your information:

**Medical Records Folder File or CHR (Consolidated Health Record):** These records contain all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a Federal records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d. (May 2016)).

**Official Human Resources Personnel File:** Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Part Two, Chapter Three-Civilian Personnel, Item No. 3000.1 (May 2016)).

**Financial Records:** Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS)-10, Part Two, Chapter Four-Finance Management (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf) for specific guidelines.

**Office if Information & Technology (OIT) Records:** These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (August 3, 2009). Please refer to VA Records Control Schedule (RCS)-05 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) for specific guidelines.

Additionally under OMB and NARA guidelines, Iowa City VA Health Care System will reference the Records Management Resources within the General Records Schedule. These specific resources can be found at http://www.archives.gov/records-mgmt/grs/.
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.

When managing and maintaining VA data and records, Iowa City VA Health Care System will follow the guidelines established in the NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)-10 (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).

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 documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans’ Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, Iowa City VA Health Care System follows Field Security Service (FSS) Bulletin for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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:

There is a risk that the information maintained by Iowa City VA Health Care System could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation:

In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

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?

INCLUDE ADDITIONAL INFORMATION BELOW AS NEEDED

<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>Department of Veterans Affairs General Counsel Office</td>
<td>Assistance in investigation of patient or employee claims</td>
<td>Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request. Patient &amp; employee name, SSN, DOB, financial information or health</td>
<td>Information transmitted upon request via electronically (email, encrypted CD’s, Fax), verbal, or written in a sentence format based upon request delivered via mail.</td>
</tr>
<tr>
<td><strong>Veterans Benefits Administration (VBA)</strong></td>
<td>Healthcare encounter information</td>
<td>Name, Date of Birth, Sex, SSN, demographics and health information</td>
<td>Information transmitted upon request via electronically (email, encrypted CD’s, Fax), verbal, or written in a sentence format based upon request delivered via mail.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>National Cemetery Administration</strong></td>
<td>Information is shared requesting verification of death benefits</td>
<td>Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request. Patient name, SSN, DOB, demographic information</td>
<td>Information transmitted upon request via electronically (email, encrypted CD’s, Fax), verbal, or written in a sentence format based upon request delivered via mail.</td>
</tr>
<tr>
<td><strong>VA Veteran Centers</strong></td>
<td>Continuity of care, eligibility, and enrollment</td>
<td>Read only access to health information for plan of treatment</td>
<td>Electronically viewed through the Computerized Patient Record System (CPRS)</td>
</tr>
<tr>
<td><strong>Health Eligibility Center (HEC)</strong></td>
<td>Healthcare encounter information</td>
<td>Name, Date of Birth, Sex, SSN, demographics and health information</td>
<td>Information transmitted upon request via electronically (email, encrypted CD’S, Fax), verbal, or written in a sentence format based upon request delivered via mail.</td>
</tr>
<tr>
<td><strong>Austin Automation Center</strong></td>
<td>Financial information for employment</td>
<td>Name, DOB, SSN, financial information</td>
<td>Information may be transmitted upon request in an electronic format.</td>
</tr>
<tr>
<td><strong>Consolidated Patient Accounts Center (CPAC)</strong></td>
<td>Healthcare encounter information for billing purposes</td>
<td>Name, Date of Birth, Sex, SSN, demographics and health information</td>
<td>Information transmitted upon request via electronically (email, encrypted CD’s, Fax), verbal, or written in a sentence format based upon request delivered via mail.</td>
</tr>
</tbody>
</table>

Facilities also internally use databases to conduct patient healthcare, tracking and analysis. This information is shared with staff on a need to know basis to fulfill job assignments. The information is typically received directly from the veteran and contains pertinent PII and PHI such as Name, Address, SSN, Date of Birth and pertinent health information.

Databases are also used to track in-bound and out-bound call traffic for telephone call centers. Information maintained includes name, phone number and call description.
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:**

The sharing of data is necessary for the medical care of individuals eligible to receive care at Iowa City VA Health Care System. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

**Mitigation:**

The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

VistA menus and security keys are assigned by an approved ePAS request based on specific job or duty requirements with least privileges. This access is reviewed for appropriateness on a quarterly basis.

VistA applies the sensitive record flag to all employees and any veteran record where the veteran requests the record be sensitized. The ISO reviews VistA audit messages for any potential access abnormalities or violations.

Iowa City VA Health Care System completes a multitude of auditing functions based on VA Handbook 6500 guidelines. Iowa City VA Health Care System completes an in-depth audit of VistA accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as adhoc reports upon request.

**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.

A list of national ISA/MOUs can be found - https://vaww.portal2.va.gov/sites/fss/CRISP-S/EAA_DOCS/Lists/System_Documents/HISD%20Documents.aspx

National Business Associate Agreements are listed here - (http://vaww.vhadataportal.med.va.gov/DataAccess/BusinessAssociateAgreements.aspx)

or additional specific, local agreements with Federal, State or local agencies as requested above

<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>Legal authority, binding agreement, SORN routine use, etc that permit external sharing (can be more than one)</th>
<th>Method of transmission and measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbott Labs</td>
<td>The VA’s Abbott Instrumentation performs routine and stat laboratory testing in chemistry, immunoassay, blood screening and hematology. Orders and results are communicated using middleware between instruments and VistA.</td>
<td>Network data could include, but is not limited to, a variety of software for services and/or the possibility of patient sensitive data. Stores PHI data but does not transmit PHI data</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Aeysnt</td>
<td>Provide pharmacy automation equipment associated implementation and maintenance services</td>
<td>Data could include but is not limited to a variety of Connect-RX automation solutions, diagnostics, software/product upgrades and/or the possibility of patient identifiable data</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Company</td>
<td>Services Provided</td>
<td>Data Collected</td>
<td>Agreement Type</td>
<td>Communication Method</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Alere Informatics, Inc.</td>
<td>Provide Healthcare technology services</td>
<td>The following data types are collected by the input devices and stored in RALS-Plus database. Name, Medical record number, account number, and blood glucose test results</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Brit</td>
<td>Provide picture archival and communications systems (PACS)</td>
<td>Data includes but is not limited to service specific data to perform remote support; incidental exposure to limited data sets with specific PHI elements depending on application such as patient name, SSN, record ID, images and gender and log files and program updates for support of the system</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>CareFusion</td>
<td>Services, support, maintenance, and data aggregation services</td>
<td>Pertinent PII, PHI, and III appropriate to the agreement; pulmonary function testing</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Department of Defense (DOD)</td>
<td>Healthcare, Benefits and Administrative Data</td>
<td>Pertinent PII, PHI, and III as appropriate to the situation</td>
<td>National ISA/MOU VA SORN 168VA10P2</td>
<td>Electronic via EDI interface /paper via US Postal Service</td>
</tr>
<tr>
<td>Federal Bureau of Investigation (FBI)</td>
<td>Background investigations</td>
<td>Pertinent PII to conduct the investigation</td>
<td>VA SORN 02VA135 VA SORN 79VA19</td>
<td>Electronic via FBI Website</td>
</tr>
<tr>
<td>Federal Emergency Management Agency (FEMA)</td>
<td>Communicate in emergency situations</td>
<td>Pertinent PII, PHI, and III as appropriate to the situation</td>
<td>VA agreement FEMA/GOFT-1 and FEMA Recovery Policy 9420.1</td>
<td>FEMA Website</td>
</tr>
<tr>
<td>GE</td>
<td>Provide medical technology through its division GE Healthcare</td>
<td>Services specific data to perform remote support, limited data sets with specific PHI elements depending on application such as patient name, DOB, Record ID, Gender, Images, and Log files and Program updates for support of the system</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Organization</td>
<td>Purpose</td>
<td>Pertinent PII</td>
<td>Agreement</td>
<td>Transmission Method</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Internal Revenue Service (IRS)</td>
<td>Communicate Veterans financial information</td>
<td>Pertinent PII to the situation</td>
<td>National ISA/MOU</td>
<td>Secure Web-Portal, Secure Socket Layer</td>
</tr>
<tr>
<td>Iowa Department of Public Health State Prescription Drug Monitoring Program</td>
<td>Provide narcotic prescription fills</td>
<td>Name, DOB, Prescription Information</td>
<td>VHA Handbook 1605-1 Release of Information</td>
<td>Website Entrust SSL File Transfer Protocol over Secure Sockets Layers</td>
</tr>
<tr>
<td>Iowa Department of Public Health</td>
<td>Medical records pertaining to state reporting requirements.</td>
<td>Name, Date of Birth, Sex, SSN, demographics and health information as indicated within the agreement.</td>
<td>VHA Handbook 1605-1 Release of Information</td>
<td>Information may be transmitted upon request in an electronic (encrypted email, fax, CD), written or verbal format based on the individual request. Secure facsimile or hard copies via routine mail. Website Entrust SSL File Transfer Protocol over Secure Sockets Layers</td>
</tr>
<tr>
<td>Merge</td>
<td>Provide professional and/or support regarding merge Healthcare software and solutions for the management of imaging and other medical data</td>
<td>Data types consist of patient ID, patient names, demographics, fundus photos, modality reports for OCT, HVFA, and other Ophthalmic diagnostic devices; DICOM images, measurements, hemodynamic data, clinical reports, AVI images, department and accreditation reports</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>NextCut Shredding</td>
<td>Data destruction vendor (i.e. paper)</td>
<td>Name, Date of Birth, Sex, SSN, demographic information, employment information, health information, medications, treatment</td>
<td>National Business Associate Agreement (BAA)</td>
<td>Data is not transmitted. Paper is shredded at shredding facility according to BAA</td>
</tr>
<tr>
<td>Office of Personnel Management (OPM)</td>
<td>Demonstrated need to know and meets</td>
<td>Name, Date of Birth, Sex, SSN, demographics and</td>
<td>National ISA/MOU</td>
<td>Information may be transmitted upon request in an</td>
</tr>
<tr>
<td>Company</td>
<td>Services Provided</td>
<td>Information Provided</td>
<td>Agreement Type</td>
<td>Communication Method</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Olympus America Inc.</td>
<td>Provide support and maintenance service, repair, trouble shooting and maintenance activities associated with the following products and their product families: EndoWorks, Endocapsule-10; nStream; and IN-10A</td>
<td>Incidental exposure to PHI, patient name, SSN, Biometric data, DOB, address, and other items from the VistA electronic health records that are used and stored on Olympus Endo Works System</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Omnicell</td>
<td>Provide medicine and supply automation support services</td>
<td>Pertinent PII, PHI and II appropriate to the agreement to provide support services and technical support</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Philips Healthcare</td>
<td>Provide healthcare technology and equipment services</td>
<td>Patient images, patient names, DOB, SSN</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Roche Diagnostics</td>
<td>Provide diagnostic instrumentation</td>
<td>PHI/PII as needed for technical support services, diagnostics and repair for Roche Medical Equipment</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>ScriptPro</td>
<td>Provide Pharmacy Technology services</td>
<td>Pertinent PII, PHI, and III appropriate to the agreement to provide support services and technical support</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Siemens</td>
<td>Provide Healthcare diagnostics solution</td>
<td>PII/PHI as needed for technical support services, diagnostics and repair for Siemens medical equipment</td>
<td>National ISA/MOU National Business Associate Agreement (BAA)</td>
<td>Electronic using Site to Site (S2S)</td>
</tr>
<tr>
<td>Social Security Administration (SSA)</td>
<td>Demonstrated need to know and meets all authorized requirements</td>
<td>Name, Date of Birth, Sex, SSN, demographics and health information</td>
<td>VHA Handbook 1605-1 Release of Information</td>
<td>Information may be transmitted upon request in an electronic (encrypted email, fax, CD), written or verbal format based on the individual request. Secure facsimile or hard copies via routine mail.</td>
</tr>
<tr>
<td>Company</td>
<td>Services Description</td>
<td>PHI/PII Details</td>
<td>Communication Method</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Sorna</td>
<td>Provide Healthcare software system</td>
<td>Software, Software updates, software code trace files, machine language trace files, network package captures, and DICOM protocol language to assist in the analysis of troubleshooting. PHI may be included in the DICOM communication.</td>
<td>National ISA/MOU National Business Associate Agreement (BAA) Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Sysmex America</td>
<td>Provide diagnostic medical equipment services</td>
<td>Data on the analyzers will include laboratory identifier number, username, full SSN, test results.</td>
<td>National ISA/MOU National Business Associate Agreement (BAA) Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Topcon Medical Systems</td>
<td>Provide ophthalmic instrumentation services</td>
<td>PHI of medical images</td>
<td>National ISA/MOU National Business Associate Agreement (BAA) Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Toshiba</td>
<td>Provide medical diagnostic imaging equipment services</td>
<td>PHI of medical images</td>
<td>National ISA/MOU National Business Associate Agreement (BAA) Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>University of Iowa</td>
<td>Medical records/treatment on Bio-Medical devices</td>
<td>Name, Date of Birth, Sex, SSN, as indicated within the agreement</td>
<td>Local ISA/MOU Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Hospitals and Clinics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University of Iowa</td>
<td>Medical records/treatment on Bio-Medical devices</td>
<td>Name, Date of Birth, Sex, SSN, as indicated within the agreement</td>
<td>Local ISA/MOU Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Hospitals and Clinics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University of Iowa</td>
<td>Medical Records as it pertains to research information</td>
<td>De-identified PII, PHI and III pertaining to research information</td>
<td>Local ISA/MOU Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
<tr>
<td>Hospitals and Clinics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vecna</td>
<td>To exchange data between DVA’s VPS VetLink Program and Vecna’s remote</td>
<td>Kiosk and Kiosk server error and performance logs, software upgrades and software</td>
<td>National ISA/MOU Electronic using Site to Site (S2S)</td>
<td></td>
</tr>
</tbody>
</table>
support services. The expected benefit of the interconnection is to expedite the processing of data associated with remote diagnostics, maintenance, monitoring and repair of VPS Kiosk application and data base servers within prescribed timelines.

patches. No PHI data will be transmitted outside of DVA owned environments. No VA sensitive information will be stored on Vecna’s systems.

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

- The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

- The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

- The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

- Internal protection is managed by access controls such as user authentication (user IDs, passwords and Personal Identification Verification (PIV)), awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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.

Privacy Risk:

The sharing of data is necessary for the medical care of individuals eligible to receive care at Iowa City VA Health Care System. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation:

The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and
communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

All personnel access to Veteran’s information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. A background investigation is required commensurate with the individual’s duties.

Individual users are only given job position specific access to individually identifying data. Access to VistA requires multi-layer authentication. The individual first must authenticate through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. VistA access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts.

**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 Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that they read and understood the NOPP is scanned into each applicant’s electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):


**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 Veterans’ Health Administration (VHA) as well as Iowa City VA Health Care System only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide the information, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Iowa City VA Health Care System.

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?

Individuals have a right to deny the use of their health information and/or Individually Identifiable Health Information (IIHI) and for the purpose of research.

Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. Iowa City VA Health Care System can approve or deny these requests. However, if the request to provide information is accepted Iowa City VA Health Care System must conform to the restrictions.

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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans’ Health Administration and Iowa City VA Health Care System prior to providing the information to the VHA.

**Mitigation:**

This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are provided to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training.
Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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/](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.*

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans’ Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at [https://www.myhealth.va.gov/index.html](https://www.myhealth.va.gov/index.html). Veterans and other individuals may also request copies of their medical records and other records containing personal data from Iowa City VA Health Care System Release of Information (ROI) office. Any individual who would like information under the Freedom of Information Act (FOIA) [5 U.S.C. 552] should contact the facility’s FOIA Officer in writing.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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._

Individuals are provided the opportunity to submit a request for change in medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the Privacy Officer at the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A decision to approve or deny is made by the practitioner who entered the data and relayed to the Veteran in writing by the facility Privacy Officer. Appeal rights are provided if a request is denied. The goal is to complete any evaluation and determination within 30 days.

_A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the Iowa City VA Health Care System_
Privacy Officer (PO), or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the Iowa City VA Health Care System business office for processing.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

**Right to Request Amendment of Health Information.**
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the Iowa City VA Health Care System ROI office.

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 ensures data accuracy.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above in Section 7.3 to request edits to their personal medical records and other personal records retained about them.

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 that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

**Mitigation:**

As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to one’s records. Beneficiaries are reminded of this information when obtaining a copy of the NOPP.

The Iowa City VA Health Care System Release of Information (ROI) office is available to assist Veterans with obtaining access to their medical records and other records containing personal information.

The Veterans’ Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy Handbook 1605.1 establishes procedures for Veterans to have their records amended where appropriate.

**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.*
Access to Iowa City VA Health Care System working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee’s functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Access is requested per Region 2 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

Access to VistA requires multi-layer authentication. The individual first must authenticate through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. VistA access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts. Once inside the system, individuals are authorized to access information on a need to know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at Iowa City VA Health Care System is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at Iowa City VA Health Care System, or an OIG office location remote from Iowa City VA Health Care System is controlled in the same manner.

Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

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.

Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). This review is conducted each time the contract period expires.

The Privacy Officer is responsible for monitoring all local contracts that require a Business Associate Agreement (BAA). The Privacy Officer will coordinate an annual review all local contracts to monitor the contractor’s compliance with the BAA.
Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

Contractors with VistA access must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees.

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 PHI are trained to handle it appropriately.

All VA employees who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the Iowa City VA Health Care System Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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.

Authority To Operate information is ongoing within Risk Vision – The most current Authority To Operate (ATO) memo is dated 4/1/15
Signature of Responsible Officials

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

Makenzie Johnson, Privacy Officer

Randall E. Smith, Information Security Officer

Robert Hensley, Information Security Officer

System Owner, Stan Bush, Director Operations, Midwest T1 for Robert L. Page, III
Director, Continental District

Makenzie Johnson, Individual Completing the PIA
Appendix A-6.1

Department of Veterans Affairs  
Veterans Health Administration  
NOTICE OF PRIVACY PRACTICES  
Effective Date September 23, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

The Department of Veterans Affairs’ (VA) Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA is also required to abide by the terms of this Notice and its privacy policies.

How VHA May Use or Disclose Your Health Information without Your Authorization (See below for more information about these categories)

- Treatment (e.g., giving information to VHA and other doctors and nurses caring for you)
- Payment (e.g., giving information to non-VHA facilities that provide care or services)
- Health Care Operations (e.g., giving information to individuals conducting Quality of Care reviews)
- Eligibility and Enrollment for VA Benefits (e.g., giving information to officials who decide benefits)
- Abuse Reporting (e.g., giving information about suspected abuse of elders or children to government agencies)
- Health or Safety Activities
- Public Health Activities (e.g., giving information about certain diseases to government agencies)
- Judicial or Administrative Proceedings (e.g., responding to court orders)
- Law Enforcement
- Health Care Oversight (e.g., giving information to the Office of Inspector General or a Congressional Committee)
- Cadaveric Organ, Eye, or Tissue Donation
- Coroner or Funeral Activities
- Services (e.g., giving information to contractors or business associates performing services for VHA)
- National Security Matters
- Workers’ Compensation Cases (e.g., giving information to officials who decide payments for workplace injuries Payment (e.g., giving information to non-VHA facilities that provide care or services)
- Correctional Facilities and/or Parole Officers
- When Required by Law
- Activities Related to Research (e.g., certain
- Planning VA research projects (e.g., investigator accesses, but does not disclose or record, individual health information to determine feasibility of opening a study)
- Military Activities (e.g., giving information to the Department of Defense (DoD)
- Academic Affiliates (e.g., giving information to assist in training medical students)
- State Prescription Drug Monitoring Program (SPDMP) reporting and query
- General Information Disclosures (e.g., giving out general information about you to your family and friends)
- Verbal disclosures to others while you are present
- Verbal Disclosures when you are not present (e.g., assisting Family Members or
Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose based on a signed, written authorization you provide us. Your signed written authorization is always required to disclose your psychotherapy notes if they exist. If we were to use or disclose your health information for marketing purposes we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Revocation of Authorization. If you provide us a written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization.

Your Privacy Rights

Right to Request Restriction.
You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, we are not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you no longer make the restriction request valid or you revoke it.

NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.
Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.

**NOTE:** Please send a written request to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is [http://www.archives.gov/veterans/military-service-records/medical-records.html](http://www.archives.gov/veterans/military-service-records/medical-records.html).

Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:

- At a mailing address (e.g., confidential communications address) other than your permanent address
- In person, under certain circumstances

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website, [http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048).

Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you should take, if any.

Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

- VA via the Internet through “Contact the VA” at [http://www.va.gov](http://www.va.gov); by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10P2C1) at 810 Vermont Avenue NW, Washington, DC 20420.
• Complaints do not have to be in writing, though it is recommended.
• An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

Changes. We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes we will make available to you a copy of the revised Notice within 60 days of any change.

When We May Use or Disclose Your Health Information Without Your Authorization

Treatment. We may use and disclose your health information for treatment or to provide health care services. Treatment may include:

• Emergency and routine health care or services, including but not limited to labs and x-rays; clinic visits; inpatient admissions
• Contacting you to provide appointment reminders or information about treatment alternatives
• Prescriptions for medications, supplies, and equipment
• Coordination of care, including care from non-VHA providers
• Coordination of care with DoD, including electronic information exchange

NOTE: If you are an active duty service member, Reservist or National Guard member, your health information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD’s access to your information in this database, even if you ask us to do so.

Examples:

1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran’s health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital that needs the information to treat this Veteran.
3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.

Payment. We may use and disclose your health information for payment purposes or to receive reimbursement for care provided, including:

• Determining eligibility for health care services
• Paying for non-VHA care and services, including but not limited to, CHAMPVA and fee basis
• Coordinating benefits with other insurance payers
• Finding or verifying coverage under a health insurance plan or policy
• Allowing you to pay for your health care out of pocket so that your insurance is not billed
• Pre-certifying benefits
• Billing and collecting for health care services provided
• Providing personal information to consumer reporting agencies regarding delinquent debt owed to VHA

Examples:
1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran’s health information to determine eligibility for health care services.

2) The VHA health care facility discloses a Veteran’s health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.

**Health Care Operations.** We may use or disclose your health information without your authorization to support the activities related to health care, including:

- Improving quality of care or services
- Conducting Veteran and beneficiary satisfaction surveys
- Reviewing competence or qualifications of health care professionals
- Providing information about treatment alternatives or other health-related benefits and services
- Conducting health care training programs
- Managing, budgeting and planning activities and reports
- Improving health care processes, reducing health care costs and assessing organizational performance
- Developing, maintaining and supporting computer systems
- Legal services
- Conducting accreditation activities
- Certifying, licensing, or credentialing of health care professionals
- Conducting audits and compliance programs, including fraud, waste and abuse investigations

*Examples:*

1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality of care review process to determine if the care was provided in accordance with the established best clinical practices.

2) A VHA health care facility discloses a Veteran’s health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.

**Eligibility and Enrollment for Federal Benefits.** We may use or disclose your health information to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service or Social Security Administration, to determine your eligibility for Federal benefits.

**Abuse Reporting.** We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

**Health and Safety Activities.** We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

**Public Health Activities.** We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. Public health activities may include:

- Controlling and preventing disease, injury, or disability
- Reporting vital events such as births and deaths
- Reporting communicable diseases such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- Tracking FDA-regulated products
- Reporting adverse events and product defects or problems
- Enabling product recalls, repairs or replacements
**Judicial or Administrative Proceedings.** We may disclose your health information without your authorization for judicial or administrative proceedings, including:

- We receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure
- To defend VA in judicial and administrative proceedings

**Law Enforcement.** We may disclose your health information to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. These law enforcement purposes may include:

- Responding to a court order
- Responding to a specific request when in pursuit of a focused civil or criminal law enforcement investigation
- Reporting crimes occurring at a VHA site
- Identifying or apprehending an individual who has admitted to participating in a violent crime
- Reporting a death where there is a suspicion that death has occurred as a result of a crime
- Reporting Fugitive Felons
- Routine reporting to law enforcement agencies, such as gunshot wounds
- Providing certain information to identify or locate a suspect, fugitive, material witness, or missing person

**Health Care Oversight.** We may disclose your health information to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

**Cadaveric Organ, Eye, or Tissue Donation.** When you are an organ donor and death is imminent, we may use or disclose your relevant health information to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for the purpose of determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

**Coroner or Funeral Services.** Upon your death, we may disclose your health information to a funeral director for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

**Services.** We may provide your health information to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contract and business associate agreement must be in place securing your information.

**National Security Matters.** We may use and disclose your health information without your authorization to authorized Federal officials for the purpose of conducting national security and intelligence activities. These activities may include protective services for the President and others.

**Workers’ Compensation.** We may use or disclose your health information without your authorization to comply with workers’ compensation laws and other similar programs.

**Correctional Facilities.** We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; to protect the health and safety of you or others; or for the safety of the facility.
**Required by Law.** We may use or disclose your health information for other purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

**Activities Related to Research.** Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

- A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.
- The IRB approves a waiver of informed consent and a waiver of authorization to use or disclose health information for the research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

**Military Activities.** We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active Duty Service members and in some cases Reservists and National Guard members. An example of a military activity includes the disclosure of your health information to determine fitness for duty or deployment to your Base Commander.

**Academic Affiliates.** We may use or disclose your health information, without your authorization, to support our education and training program for students and residents to enhance the quality of care provided to you.

**State Prescription Drug Reporting Program (SPDMP).** We may use or disclose your health information, without your authorization, to a SPDMP in an effort to promote the sharing of prescription information to ensure appropriate medical care.

**General Information Disclosures.** We may disclose general information about you to your family and friends. These disclosures will be made only as necessary and on a need-to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- Verification of identity
- Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- Your location in a VHA health care facility (e.g., building, floor, or room number)

**Verbal Disclosures to Others While You Are Present.** When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. For example, your doctor may talk to your spouse about your condition while at your bedside. Before we make such a disclosure, we will ask you if you object. We will not make the disclosure if you object.
**Verbal Disclosures to Others When You Are Not Present.** When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person’s involvement with your health care or payment for your health care.

Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

**IMPORTANT NOTE:** A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care only if we have your signed, written authorization or if the individual is your authorized surrogate (the individual who is authorized to make health care decisions on your behalf if you can no longer do so) and the practitioner determines that the information is needed for the individual to make an informed decision regarding your treatment.

**When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information**

**Patient Directories.** Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name. If you do object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.

**When We Will Not Use or Disclose Your Health Information**

**Sale of Health Information.** We will not sell your health information. Receipt of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA fees is not a sale of health information.

**Genetic Information Nondiscrimination Act (GINA).** We will not use genetic information to discriminate against you either through employment or to determine your eligibility for VA benefits.

**Contact Information.**

You may contact your VHA health care facility’s Privacy Officer if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Informatics and Analytics (10P2C1), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038.

**NOTE:** A large print version of this Notice is available upon request from the facility where you are receiving