Privacy Impact Assessment for the VA IT System called:

# Healthcare Safeware -E

# Veterans Health Administration

# South Texas Veterans Healthcare System (STVHCS)

# eMASS ID#:2533

Date PIA submitted for review:

3/14/2025

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nigel Burns | Nigel.Burns@va.gov | 210-616-8286 |
| Information System Security Officer (ISSO) | Martin DeLeo | Martin.DeLeo@va.gov | 202-299-6495 |
| Information System Owner | Aimee Barton | Aimee.Barton@va.gov | 216-707-7726 |

## Abstract

*The abstract provides the simplest explanation for "what does the system do for VA?".*

The Healthcare Safeware -E system will help advance workflow and analyze records to output actionable data for the providers and facility. It is designed for frontline staff to review cases for hidden opportunities for improvement in care to be identified, recorded, and reported with greater accuracy. The software aims to reduce mortality rates and delivery higher quality, timely, cost-effective care.

## Overview

*The overview is the most important section of the Privacy Impact Assessment (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:*

*1 General Description*

*A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

The Healthcare Safeware -E software will help STVHCS in their mission to improve delivered care while decreasing the rate of system errors and reducing the overall probability of patient mortality.

*B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA Controlled / non-VA Owned and Operated

*2. Information Collection and Sharing*

*C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

100 veterans per year plus 20 internal users.

| Check if Applicable | Demographic of individuals |
|---|---|
| ☒ | Veterans or Dependents |
| ☒ | VA Employees |
| ☒ | Clinical Trainees |
| ☒ | VA Contractors |
| ☐ | Members of the Public/Individuals |
| ☐ | Volunteers |

*D. What is a general description of the information in the IT system and the purpose for collecting this information?*

The system will process de-identified patient data, such as length of stay, sex, advance directives, diagnoses, patient location, patient disposition and other contributing factors. This information will be reviewed and used to pinpoint common causes of patient harm in the facility's systems and processes and provide solutions to address these failures of care delivery.

*E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The IT system does not share PII or PHI externally. Only VA users have access to PII/PHI.

F. Are the modules/subsystems only applicable if information is shared?

No

*G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

No

*3. Legal Authority and System of Record Notices (SORN)*

*H. What is the citation of the legal authority and SORN to operate the IT system?*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.
Patient Medical Records-VA- 24VA10A7/ 85 FR 62406
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

*I. What is the SORN?*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.
Patient Medical Records-VA. - 24VA10A7/ 85 FR 62406
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

*J. SORN revisions/modification*

No revisions/modifications needed.

*K. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No

*4. System Changes*

*L. Will the business processes change due to the information collection and sharing?*

☐ *Yes*
☒ *No*
*if yes, <<ADD ANSWER HERE>>*

*M. Will the technology changes impact information collection and sharing?*

☐ *Yes*
☒ *No*
*if yes, <<ADD ANSWER HERE>>*

## 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 Information 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 VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). 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.*

*This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.*

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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
- ☐ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☒ Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI) ☒ Other Data Elements (list below)

Other PII/PHI data elements: Encounter Number, Name of clinical specialty, Clinical Summary Notes, Opportunity for Improvement data (date, time, location), Unique Case ID – Number randomly generated to each case

**1.2 List the sources of the information in the system**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?*

The information is collected by reviewing CPRS and VISTA and manually entered in the system.

*1.2b 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*

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

*public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.*

The data is only taken from internal VA sources. This is usually mortality review. Any patients identified would come from internal VA systems.

*1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?*

The system does not create its own information.

**1.3 Methods of information collection**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.3a 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 technologies used in the storage or transmission of information in identifiable form?*

No, information is not collected or transmitted in identifiable form.

*1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?*

Information is not collected on a paper form.

**C1.4 Information checks for accuracy, and how often will it be checked.**

*These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

*1.4a Discuss whether and how often 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? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

There is no automated quality assurance. Accuracy is dependent upon the VA user entering the data and reviewing.

*1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?*

No, the system does not check for accuracy by accessing a commercial aggregator of information.

**1.5 Identify the specific legal authorities, arrangements, and agreements that 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. This question is related to privacy control AP-1, Authority to Collect*

Patient Medical Records-VA. MOU. The Privacy Act, 5 U.S.C. § 552a, implemented by 38 C.F.R. §§ 1.575-1.582.

P.L. 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA).

**1.6 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.* (*Work with your System ISSO to complete this section)*

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

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

*Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.*

*Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.*

*Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
*This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.*

Follow the format below when entering your risk assessment:

**Privacy Risk:**
The system collects & processes PII and PHI on Veterans. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

**Mitigation:** Veterans Health Administration (VHA) 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 VHA to 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.

## 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 that 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. This question is related to privacy control AP-2, Purpose Specification.*

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Medical Record Number | Patient Identification | Not Available |
| DOB | Patient Identification | Not Available |
| Encounter Number | Patient Identification | Not Available |
| Medical Records | Patient Identification | Not Available |
| Sex | Patient Identification | Data Analysis/Benchmarking |
| Name of clinical specialty | Understand clinical encounter | Understand clinical encounter |
| Clinical Summary Notes | Understand clinical encounter | Understand clinical encounter |
| Opportunity for Improvement data (date, time, location) | Understand clinical encounter | Understand clinical encounter |
| Unique Case ID – Number randomly generated to each case | Not used | Case identification |

**2.2 Describe the types of tools used to analyze data and what type of data may be produced.**
*These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.*

*2.2a 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?*

Pareto charts, Pie charts, bar charts etc used for summary analysis.

*2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

The system does not create or make new or previously unutilized information.

**2.3 How the information in the system is secured.**
*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

*2.3a What measures are in place to protect data in transit and at rest?*

Data is encrypted in rest and in transit.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).*

No SSNs are collected, processed, or retained.

*2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?*

The Privacy Act, 5 U.S.C. § 552a, implemented by 38 C.F.R. §§ 1.575-1.582.

The system is architected and completely complies with NIST 800-53 revision 5 for security and privacy. NIST compliant means that all PII/PHI listed above is compliant with the controls that are operational, technical, and management per standards and guidelines information systems use to maintain confidentiality, integrity, and availability.

**2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>**

*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:*

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

*<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?*
*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

*2.4a How is access to the PII determined?*

VHA Directive 1605.2 - "Minimum Necessary Standard for Access, Use, Disclosure and Requests for PHI This directive updates the policy for determining the minimum necessary amount of PHI that VHA personnel may access, use, disclose, or request and requires the assignment of functional categories to all VHA personnel. This ensures that all VHA personnel understand an are aware of their obligation to only access the minimum data necessary to conduct their official job duties. Functional categories are not synonymous with access controls or menu assignment trees. Functional categories are specific definitions of types of job functions and the corresponding minimum amount of PHI data necessary to perform that function.

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?*

Yes, access is determined on a case-by-case basis. Users will have access assigned to them. VHA Directive 1605.2 - "Minimum Necessary Standard for Access, Use, Disclosure and Requests for PHI

*2.4c Does access require manager approval?*

Yes

*2.4d Is access to the PII being monitored, tracked, or recorded?*

System Administrator is responsible for tracking and monitoring all access in the system. Users will only have access to need-to-know information which is controlled within their role assignment.

*2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?*

Information System Security Officer (ISSO) and Program Manager

## 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. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Name
DOB
Medical Records
Race/Ethnicity
Medical Record Number
Sex
Date of Death
Encounter Number, Name of clinical specialty, Clinical Summary Notes, Opportunity for Improvement data (date, time, location), Unique Case ID – Number randomly generated to each case

**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.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

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)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d.

**3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).**

*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. Please work with the system VA Records Officer to answer these questions.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

*3.3a Are all records stored within the system of record indicated on an approved disposition authority?*

Yes

*3.3b Please indicate each records retention schedule, series, and disposition authority?*

Records Control Schedule 10-1 https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
Item number 6000.2a2 - Interim Electronic Source Information - Disposition Authority N1-15-02-3, item 2

Records Control Schedule 005-1 http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

**3.4 What are the procedures for the elimination or transfer of SPI?**

*Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory 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.? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information within the Area San Antonio is destroyed by the disposition guidance of. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. 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. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1.

**3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?**

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.*

Yes, PII is not used in testing, training, or research.

**3.6 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).*

*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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

*Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:

**Privacy Risk**: There is a risk that the information maintained by Healthcare Safeware -E system will 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 in Healthcare Safeware -E system 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/Receiving/Transmitting and Disclosure

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

**PII Mapping of Components**

4.1a Healthcare Safeware -E consists of 0 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Healthcare Safeware -E and the reasons for the collection of the PII are in the table below.

**Note**: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

*Internal Components Table*

| Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A | N/A |
| | | | | | |

**4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.**

**NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.**

*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 data elements (PII/PHI) are 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?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| N/A | N/A | N/A | N/A |
| | | | |

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

*Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).*

*This question is related to privacy control UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** No risk is presented as there is no internal sharing.

**Mitigation:** Mitigation is not needed, as no risk is presented.

## Section 5. External Sharing/Receiving 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.**

**The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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.**

**NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

*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 data elements (PII/PHI) are 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.*
*This question is related to privacy control UL-2, Information Sharing with Third Parties*

*Data Shared with External Organizations*

| ***List IT System or External Program Office information is shared/received with*** | ***List the purpose of information being shared / received / transmitted*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)*** | ***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|
| HB Healthcare Safeware Saas Web Portal | Patient Care | • Medical Record Number<br>• DOB<br>• Medical Records<br>• Sex<br>• Contributing human factors data<br>• Name of clinical specialty<br>• Clinical Summary Notes<br>• Opportunity for Improvement data (date, time, location) | MOU/ISA E-5444 | Data is encrypted in rest and in transit. The system is architected and completely complies with NIST |

| | | | | |
|---|---|---|---|---|
| | | • Unique Case ID – Number randomly generated to each case | | 800-53 revision 5 for security and privacy. |
| | | | | |

**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.*

*If no External Sharing listed on the table above,* ***(State there is no external sharing in both the risk and mitigation fields).***

*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.*
*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** The sharing of data is necessary to identify opportunities for improvement within the cohort of data being reviewed. There is a risk as with any web-based software that there could be a data breach.

**Mitigation:** Safeguards have been put in place to ensure data is not breached or shared inappropriately with any organization. Employee security and privacy training and awareness and use of single sign on process in conjunction with Personal Identification Verification (PIV) cards, Personal Identification Numbers (PIN) encryption and access authorization are all measures that are utilized within the administrations. Data is encrypted in rest and in transit. The system is architected and completely complies with NIST 800-53 revision 5 for security and privacy.

## 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms,**

**notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**

*These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

*6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

Privacy Act and HIPPA information provided to all patients.
*https://www.va.gov/south-texas-health-care/policies/*
*file:///C:/Users/VHASTX~2/AppData/Local/Temp/1/MicrosoftEdgeDownloads/9112e153-b08e-4cca-a322-ad390b8684e7/1605_04_D_2024-02-12.pdf*

*6.1b If notice was not provided, explain why.*

Notice was provided.

*6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.*

Posted throughout the facility and given to patients.

**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. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.*

No there is no option to decline.

**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? This question is related to privacy control IP-1, Consent.*

As per VHA Directive 160504 Notice of Privacy Practices, the Utilization of privacy policy and applicable HIPPA laws. Public Law 104-191 implemented by CFR parts 160 and 164, statue provides for the improvement of the efficiency and effectiveness of the health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, and security of certain health information.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).*

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

*Principle of Transparency: This is referring to sufficient notice provided to the individual.*

*Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.*
*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** There is a risk that Veterans and other members of the public will not know that the STVHCS exists or that it collects, maintains, and analyzes PHI/PII about them.

**Mitigation:** The risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for healthcare. Employees and contractor 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 (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the overview section of this PIA.

## 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 The procedures that allow individuals to gain access to their information.**

*These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

*7.1a 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

eMass System ID#2533 Systems and Services Acquisition (SA) Policy and procedures for allowing access to the SLS system.

*7.1b 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)?*

The Privacy Act exemption SOR Number 24VA10A7/85 FR 62406 Patient Medical Records VA. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

*7.1c 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?*

System is a Privacy Act system.

**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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Information in the system is not accessible by patients. Any erroneous information found in the system by the user that needs to be corrected they would contact Jennifer McElroy, 210-279-3855, or email Jennifer.mcelroy@va.gov.

**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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Information in the system is not accessible by patients. Any erroneous information found in the system by the user that needs to be corrected they would contact Jennifer McElroy, 210-279-3855, or email Jennifer.mcelroy@va.gov.

**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.***
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Access is not granted to individuals for this system.

**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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

*Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*
*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that Veterans and other members of the public will not know that the STVHCS exists or that it collects, maintains, and analyzes PHI/PII about them.

**Mitigation:** The risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for healthcare. Employees and contractor 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 (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the overview section of this PIA.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

**8.1 The procedures in place to determine which users may access the system, must be documented.**

*These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

*8.1a Describe the process by which an individual receives access to the system?*

Access to the system is granted per established SOP by the system administrator.

*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Users from other agencies do not have access to the system.

*8.1c 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.*

User roles are defined within the system and are granted based on the SOP and need to know.

**8.2a. Will VA contractors have access to the system and the PII?**

No

**8.2b. What involvement will contractors have with the design and maintenance of the system?**

Cloud server storage and general systems helpdesk.

**8.2c. Does the contractor have a signed confidentiality agreement?**

Yes

**8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?**

Yes

**8.2e. Does the contractor have a signed non-Disclosure Agreement in place?**
*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. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes

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

*VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.*

Privacy Awareness and Training, HIPPA yearly training.

**8.4 The Authorization and Accreditation (A&A) completed for the system.**

Yes

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 10/14/2024
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 10/18/2024
5. *The Authorization Termination Date:* 04/16/2025
6. *The Risk Review Completion Date:* 10/18/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

*Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.*

*8.4b If No or In Process, provide your* ***Initial Operating Capability (IOC) date.***

A Sponsored FedRAMP ATO process is the initial A&A process for the Healthcare Safeware -E SaaS application and is In Process. The following items are included in this process: Security Plan, Authorization, and Risk Review. The estimated IOC date is 2/19/2025. The system is currently classified as Moderate Impact.

## Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

**9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.* ***(Refer to question 1.8 of the PTA)***

This system is a Software as a Service (SaaS) that uses cloud technology. There is no current agency authorization or FedRAMP Authorization for the solution, but it is currently in process of pursuing a VA-Sponsored FedRAMP Authorization. The system has a current data security categorization of Moderate from VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office.

**9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

There is no contractual agreement between the VA and the CSP. The agreement is between the VA and the SaaS solution vendor Healthcare Safeware. However, the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is 36C10A22C0006.

**9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?**

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

No

**9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

As detailed in the contract security and privacy of the data defines the roles and responsibilities of the VA and HB Healthcare.

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

*Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).*

The system does not use RPA.

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

| ID | Privacy Controls |
|---|---|
| **AP** | **Authority and Purpose** |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| **AR** | **Accountability, Audit, and Risk Management** |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-7 | Privacy-Enhanced System Design and Development |
| AR-8 | Accounting of Disclosures |
| **DI** | **Data Quality and Integrity** |
| DI-1 | Data Quality |
| DI-2 | Data Integrity and Data Integrity Board |
| **DM** | **Data Minimization and Retention** |
| DM-1 | Minimization of Personally Identifiable Information |
| DM-2 | Data Retention and Disposal |
| DM-3 | Minimization of PII Used in Testing, Training, and Research |
| **IP** | **Individual Participation and Redress** |
| IP-1 | Consent |
| IP-2 | Individual Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| **SE** | **Security** |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| **TR** | **Transparency** |
| TR-1 | Privacy Notice |
| TR-2 | System of Records Notices and Privacy Act Statements |
| TR-3 | Dissemination of Privacy Program Information |
| **UL** | **Use Limitation** |
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

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

NIGEL BURNS Digitally signed by NIGEL BURNS
Date: 2025.06.09 12:03:18 -05'00'

**Privacy Officer, Nigel Burns**

JOHN DELEO Digitally signed by JOHN DELEO
Date: 2025.06.09 13:25:55 -04'00'

**Information Systems Security Officer, Martin DeLeo**

AIMEE BARTON Digitally signed by AIMEE BARTON
Date: 2025.07.09 17:06:02 -04'00'

**Information Systems Owner, Aimee Barton**

## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

## HELPFUL LINKS:

**Records Control Schedule 10-1 (va.gov)**

**General Records Schedule**
https://www.archives.gov/records-mgmt/grs.html

**National Archives (Federal Records Management):**
https://www.archives.gov/records-mgmt/grs

**VA Publications:**
https://www.va.gov/vapubs/

**VA Privacy Service Privacy Hub:**
https://dvagov.sharepoint.com/sites/OITPrivacyHub

**Notice of Privacy Practice (NOPP):**
VHA Directive 1605.04
IB 10-163p (va.gov)