Privacy Impact Assessment for the VA IT System called:

Enterprise Cloud Fax Government -E

Department of Veterans Affairs Corporate Office (VACO)
Infrastructure Operations (IO)
Office of Information and Technology (OIT)

Application cloud and Edge Solutions (ACES) Platform Management Product Line

Content Hosting and Delivery Solutions (CHDS)

Date PIA submitted for review:

June 22, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov; oitprivacy@va.gov	202-632-8423
Information System Security Officer (ISSO)	Scott Miller	Scott.Miller@va.gov	717-413-1940
Information System Owner	Frank Joy, Jr.	Frank.Joy@va.gov	210-694-6352

Abstract

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

This IT System implements an enterprise wide, commercial off-the-shelf, cloud-based, scalable, secure, digital Software as a Service (SaaS) fax/data transfer managed service, which is able to: Reduce the number of faxing related service contracts from over 150 to just a single unified vendor; interface with Microsoft Office 365/Outlook, Electronic Health Records Management (EHRM), Multifunction Devices (MFD) and other Workstreams; support customer business requirements through multiple means of delivery; and further secures Veterans Administration (VA) Personal Identifying Information (PII) and Protected Health Information (PHI).

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:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The IT System name is "Enterprise Cloud Fax Government -E". The referential acronym of which is "ECFax". The system is actively managed by Infrastructure Operations, Platform Management Office of Information and Technology (OIT)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

This IT System is a scalable, secure digital fax/data transfer system. VA OIT recommended in March 2018 that VA implement an enterprise-wide, scalable, secure, managed cloud based electronic SaaS fax system for increased efficiency, security, and decrease the time and cost associated with manual faxing.

C. Indicate the ownership or control of the IT system or project.

The system is owned and operated by Consensus Cloud Solutions, Inc. and Cognosante, LLC, on behalf of VA as the Cloud Service Provider (CSP).

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

This system is expected to be utilized by all Veterans Affairs Organizations, and therefore will temporarily store and transmit information about approximately 30,000,000 individuals. The typical affected individual is a United States Military veteran or their dependent or survivors.

E. A general description of the information in the IT system and the purpose for collecting this information.

- Names
- Date of Birth
- Mother's Maiden name
- Personal Email address
- Personal Mailing address
- Personal Phone Numbers
- Emergency contact information (Name, Phone Number, et cetera)
- Financial Account Information
- Geographic Subdivisions smaller than a state
- All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age
- Telephone numbers
- Fax numbers
- Social security numbers
- Race/Ethnicity
- Gender
- Integration Control number
- Military History/Service Connection
- Next of Kin
- Medical records numbers
- Current Medications
- Previous Medical Records
- Health Plan Beneficiary Account numbers
- Account numbers
- Tax Identification Number
- Certificate/License numbers
- Vehicle identifiers and serial numbers including license plate numbers
- Device identifiers and serial numbers
- IP Address number
- Device identifiers
- Biometric identifiers
- Full face photographic images and comparable images
- Any other unique identifying number, characteristic, or code

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

The system processes and transmits information internally with a variety of VA systems including Veterans Benefit Management System (VBMS) to communicate with individuals about benefits; Veterans Health Information System Technology Architecture (VistA) imaging system to manage and communicate Electronic Health Records to VAMCs, CBOCs, and other healthcare providers, healthcare billing agencies and clearinghouses, benefit examination doctors, and pharmacies. The system also processes or transmits information with a variety of other systems including those utilized by Veterans Services Organizations; contractors and vendors; American Red Cross and other blood suppliers; learning institutions including colleges, universities, and trade schools; local, state, Federal and Tribal government agencies; attorneys; state and Federal prisons; and the general public. The purpose of sharing this information is to manage and execute all required communication regarding a veteran's benefits, status, and other relevant information managed by VA

regarding a veteran or their dependents and survivors, as required or allowed by regulation or legislation.

G. Whether the system is operated in more than one 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.

The system as a Cloud based SaaS product resides a secure instance of AWS GovCloud environment with appropriate backup capabilities for disaster recovery capabilities.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

This system operates under provisions of 5 U.S. Code § 301; 44 U.S. Code § 3101 which authorizes the head of an Executive department or military department to prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property as well as make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. This does not authorize withholding information from the public or limiting the availability of records to the public. Faxed information via this system provides for and supports these necessary government functions. SORN 90VA194 Call Detail Records – VA.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

A SORN exists and will require amendment or revision and approval. The SORN will be amended to cover cloud usage and storage of system metadata.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

The completion of this PIA will result in circumstances that require changes to business processes, specifically the management of fax/data transmission electronically including managed and fully automatic delivery to addressee individuals and groups as opposed to manual management as is the current standard. This will also remove the need for manual time-stamping receipt of documentation as this will be fully automated.

K. Whether the completion of this PIA could potentially result in technology changes

The completion of this PIA will result in technology changes through introducing electronic fax/data transmission to all VA organizations, including integration of some existing faxes, printers, and multi-function devices as well as on-premises software and SaaS systems.

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 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.

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
☒ 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*
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Geographic Subdivisions smaller than a state
All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age
Telephone numbers
Biometric identifiers
Full face photographic images and comparable images
Any other unique identifying number, characteristic, or code
Device identifiers and serial numbers

*Any type of Certificate/License numbers

PII Mapping of Components (Servers/Database)

Enterprise Cloud Fax Government consists of 10 components operating as a unified Software as a Service (SaaS capability hosted in a secure cloud-based environment). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise Cloud Fax Government 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
Amazon Web Service (AWS) GovCloud	Yes	Yes	• Names • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers	Hosting location of a variety of SaaS solutions utilized by VA for information management and storage	Encrypted both in transit and at rest with FIPS 140-2 (or its successor) both inbound and outbound

			• Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		
Veterans Benefits Management System (VBMS) – (Interconnection intended for future implementation).	Yes	Yes	• Names • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers	Benefit management	Encrypted both in transit and at rest with FIPS 140-2(or its successor) both inbound and outbound

			• Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers		

			• Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		
VistA/Cerner - (Interconnection intended for future implementation).	Yes	Yes	• Names • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number	Electronic health record management	Encrypted both in transit and at rest with FIPS 140-2 (or its successor) both inbound and outbound

			• Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		
VAEC Microsoft Azure - (Interconnection intended for future implementation).	Yes	Yes	• Names • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information	Information potentially stored related to VA email accounts, a primary fax/data transmission source and destination	Encrypted both in transit and at rest with FIPS 140-2 (or its successor) both inbound and outbound

			• Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers		

			• Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		
Dependent upon Organization Requirements - (Reserved for future necessary interconnections for future implementation).	Yes	Yes	• Names • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers	VA organization data and information management systems	Encrypted both in transit and at rest with FIPS 140-2(or its successor) both inbound and outbound

			• Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		

1.2 What are 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 PII/PHI is transmitted by the system user in the form of information contained within an electronic fax.

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 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.

No sources other than fax sender either for an individual or from any of the above listed organizations are required.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The ECFax will provide data sources for a future capability for a centralized management portal for viewing of aggregate service process which will be limited to use of service metadata for aggregate usage metrics tracking and reporting. No individually processed data contained in a fax transmission will be available for viewing or analysis beyond basic metadata.

1.3 How is the information collected?

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?

The data is provided by users of the system in three ways: 1) by VA users when establishing accounts within the ECFax system, 2) contained within the documents to be transmitted when sending faxes via the system, and 3) contained within the documents to be transmitted to users when received via the syst

1.3b 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 is not collected on a form.

1.4 How will the information be checked for accuracy? 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.

Fax Content: Faxes that are transmitted into and from the ECFax Service are temporarily uploaded to the service's secure storage area "as is" without verifying their accuracy or timeliness prior to final transfer to the intended destination. Instead, the underlying faxed information transmitted and received by the service used by both the VA and other activities must be validated by the end recipients for accuracy and completeness.

Sender/Recipient Data: ECFax users are responsible for ensuring that all data content to be faxed is accurate when entering it into the system including the source and destination address. The VA relies on the vendor to maintain accurate user metadata pertaining to senders and recipients for review and audit

1.4b 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.

The system does not check for accuracy by accessing a commercial aggregator of information.

1.5 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. This question is related to privacy control AP-1, Authority to Collect

This system operates under provisions of 5 U.S. Code § 301; 44 U.S. Code § 3101 which authorizes the head of an Executive department or military department to prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property as well as make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. This does not authorize withholding information from the public or limiting the availability of records to the public. Faxed information via this system provides for and supports these necessary government functions. SORN 90VA194 Call Detail Records – VA.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?

<u>Principle of Individual Participation:</u> 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 VA to ensure that personally identifiable information is accurate, complete, and current?
This question 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:
This system provides the ability to electronically send and receive faxed documents that may contain PHI/PII or other sensitive information. Therefore, the risk of either deliberate or inadvertent release or capture of information related to users of the system both internal and external to the service represent a high level of privacy impact. The system can be used to transmit and receive faxed data from every part of the VA to support the agency's needs in meeting all VA missions. The potential exists for the system to be used to communicate the most sensitive data the VA maintains.

Information types that include PII and/or PHI as documented in the PTA and PIA must be protected in compliance with provisions of the Privacy Act of 1974 and with the Health Insurance Portability and Accountability Act of 1996, respectively.

Another important consideration is the large quantity of records shared and the aggregate impact that a failure to maintain protection of those records could have on large numbers of the population served by the VA. Additional potential impact would be to the reputation of VA and the public trust that is required for VA to fulfill its mission in an effective manner.

There is no way to control what type and classification of data the end users of the system will be transmitting from within the VA. Additionally, external entities will be sending data to VA and there will be no way to control the content of the data being transmitted to the VA.

Individually, the system could be used for health care delivery services providing and supporting the delivery of health care to VA beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation. As noted, other sensitive information may include strategic planning information, law enforcement data as well as funding and other financial instruments.

Mitigation:
This system will employ several technical and user capabilities to support mitigation of these potential privacy impact issues.

The ECFax system internally requires all information to be encrypted from end to end both in transit and at rest. In addition, the faxing data storage of uploaded materials is temporary. After the system transmits the fax, confirms its receipt by the recipient(s), and notifies the VA sender that the fax has been received by its intended recipient(s), the system automatically and securely and deletes the faxed materials from its system. This process applies regardless of direction of transmission and must use government approved encryption methods. All external telecommunications must remain unencrypted at the service edge to ensure successful processing.

There is a risk that users may inadvertently transfer sensitive data (including Sensitive PII) to unintended recipients, but this risk also exists with manual fax transmission. This risk is addressed by administrative

and technical controls adopted by the VA as well as security and process control inherent in the ECFax service.

Furthermore, all VA users are instructed to verify that the recipient fax number(s) that appear in a confirmation box on the user's screen are correct before the fax can be sent from the system, and after the fax is sent, the user receives e-mail confirmation that the fax was sent and may verify that the fax was sent to the correct recipient.

To prevent VA users and administrative users from exceeding their authorized access and viewing documents or files from other accounts VA users cannot access other accounts and system administrators do not have access to files that have been transmitted by the system. Administrators have access to information about which senders have sent faxes on which days for auditing, access control, and billing purposes.

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

Names: Used to identify authorized account holders in the ECFax system. May also be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Mother's Maiden Name: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Personal Telephone numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Personal Mailing address: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Personal Email address: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Financial Account Information: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Geographic Subdivisions smaller than a state: City, Zip Code, and Street address may be collected as part of authorized user contact information in the system, though they are not required. This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Telephone numbers: Fax and contact phone numbers for authorized users of the ECFax system are stored, as are the fax numbers for all sent and received faxes. This type of data may also be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Fax numbers: Fax phone numbers associated with authorized users of the ECFax system are stored, as are destination fax numbers for all transmitted and received faxes. This type of data may also be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Social Security numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Race/Ethnicity: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Gender: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Integration Control number: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Military History/Service Connection: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Next of Kin: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Medical records numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Current Medications: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Previous Medical Records: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Health plan beneficiary numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Account numbers: Account numbers identifying every account in the ECFax system are stored in the system. This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Certificate/License numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Vehicle identifiers and serial numbers including license plate numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Device identifiers and serial numbers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Web URLs: This type of data may be stored in the ECFax system to identify webhook URLs for authorized API users, if selected. This type of data may also be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

IP Address number: This type of data may be stored identifying "whitelisted" IP Addresses for web or email traffic for a given user, and also potentially to identify traffic sources sending fraudulent or abusive traffic to the system in order to restrict or allow traffic originating from specific IP Addresses. This type of data may also be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Biometric identifiers: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Full face photographic images and comparable images: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

Any other unique identifying number, characteristic, or code: This type of data may be contained in any fax transmitted or received by the system for a virtually unlimited number of reasons.

2.2 What types of tools are 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.

This system primarily only processes and transmits the fax data content. It doesn't have the ability to change, capture, or store directly any of the faxed data regardless of direction (inbound or outbound) of the faxed documents. Secondarily, the system generates metadata to track the fax transmission from first contact to delivery.

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.

ECFax will not create new or previously utilized information on any individuals. The service only processes and transfers the faxed data to either the inbound or outbound destination. Based on the specific

business user the receive faxed transmission may be uploaded into a individuals record or used to determine outcomes for care and benefits, process invoices, and other use cases as defined in this PIA. Faxed documents will be delivered to VA destinations as defined by the specific business users' requirements. Once delivered, the faxed documentation and its protection and processing is the sole responsibility of the receiving activity.

2.3 How is the information in the system 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?

All fax file media and metadata are protected in transit and at rest by encryption based on FIPS 140-2 or its successor.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The system does not explicitly collect, process, or store SSNs. It is possible that SSNs are included in any given fax document transmitted or received by the system. These incidental SSNs are protected by the standard protection of data: All fax file media and metadata are protected in transit and at rest by government approved and validated encryption.

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

The system does not explicitly collect, process, or store PII except as discussed in section 2.1, above, nor does it explicitly collect PHI. However, it is possible that PII and PHI are included in any given fax transmitted or received by the system. This incidental PII and PHI is protected by the same mechanism: all fax document media is protected in transit and at rest by encryption. Furthermore, the faxes sent and/or received by a given authorized user of the system are only able to be viewed by that authorized user or other authorized users assigned to the same account by an authorized account administrative use

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. ***<u>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.</u>***

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?

The system does not explicitly collect, process, or store PII except as discussed in section 2.1, above, nor does it explicitly collect PHI. However, it is possible that PII and PHI are included in any given fax document transmitted or received by the system. This incidental PII and PHI is protected by the same mechanism: all fax document media is protected in transit and at rest by government approved encryption.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. Faxed documents sent by an authorized user of the system are only able to be viewed by that authorized user as determined by the using business entity or other users assigned to the same document delivery repository as determined by the business process owner.

2.4c Does access require manager approval?

Yes. Access to any PII or PHI are included in faxed documents sent and/or received by an authorized user of the system, with the authorized user account being assigned only with appropriate permissions granted by authorized personnel.

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

No, the ECFax service once it has delivered or transmitted the faxed documents has no tracking mechanism for any fax that may have contained PHI/PII. Transmission and processing of faxed data is the sole responsibility of the user of the service.

2.4e Who is responsible for assuring safeguards for the PII?

ECFax only processes and transfers the faxed data to either the inbound or outbound destination. Faxed documents will be delivered to VA destinations as defined by the specific business users' requirements. Once delivered, the faxed documentation and its protection and processing including all PII is the sole responsibility of the receiving activity. The ECFax service does provide a standard Privacy/HIPPA fax coversheet for use by all VA users of the service to ensure that all fax transmission destinations are aware of the potential content and requirement to protect the data received.

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

PHI/PII Listed in question 1.1 relating to authorized users (Name, Address, Email, Fax, and Phone Numbers) is retained by the system if a user is recorded in the system. Fax media files may potentially contain any or all PII and PHI identified in Section 1.1 and will be retained in the ECFax system as follows: for received faxes, until such time as the delivery of the fax file has been affirmed by the recipient; both sent and received fax files may be retained in the ECFax system for any a maximum of 5 retires to send to the destination based on direction. In the event of failure, the user is notified, and the fax data is purged from the service, only the call detail metadata will remain.

The following call detail metadata is retained by the system for administration and support purposes:

Type	**Purpose**
MESSAGEID	Message Identifier
USAGEDATETIME	Transmission Date/Time
CUSTOMERKEY	Key identifying customer
DURATION	Number of seconds of fax transmission time
PAGES	Number of pages transmitted
FAX_FROM_NUMBER	Number the fax came from
FAX_TO_NUMBER	Number the fax was directed to
CSID	Called subscriber identification (feature of fax protocol) When a fax transmission occurs, the CSID (receiving fax machine's information) is transmitted to the sending machine. This information can be used in confirmation pages and fax logs.
CALLERID	Caller Id (feature of telephony protocol)
STATUS	Whether the fax was successful or failed
RETRIES	Number of retries attempted

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? This question is related to privacy control DM-2, Data Retention and Disposal.*

All non-user data stored in the system is comprised of unstructured data contained within fax files and the metadata relating to those files' transmission or reception. The retention of fax media files is controlled by the system and is set for purge once the faxed data has successfully completed transmission or purged

after 5 retry attempts at transmission. The fax call detail metadata is retained for administrative and billing support purposes only

3.3 Has the retention schedule been 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. 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.
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?

This system will use the following NARA general records schedule. 5.5 Mail, Printing, and Telecommunication Service Management Recordshttps://www.archives.gov/files/records-mgmt/grs/grs05-5.pdfDisposition Authority DAA-GRS-2016-0012-0001

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

The call detail meta data under this schedule is classified as Temporary. It will be destroyed when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use.

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.

There is no physical data retained by the ECFax system. Electronic data stored in the ECFax system database is deleted and rendered irretrievable by subsequent queries the overwrite the previous data. All media files stored to disk or storage subsystem are deleted via a specific internal process that results in the successive overwrite of the faxed data. Only the call detail meta data is retained for the specific disposition period as noted in section 3.3

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.

The system does not use PII for research, testing, or training of new application features for deployment.

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 ISSO 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: 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?
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: The privacy risk of retention of data in the system is low. As noted in section 3.1-3.4 the system automatically deletes both transmitted fax data and fax data that in unsuccessful. The only data retained is the call detail metadata for administrative purposes as noted.

Mitigation: As noted above, the ECFax system has technical and operational capabilities to implement the data management features as noted.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

NOTE: Question 3.9 (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.

This system is expected to be utilized by all U.S Department of Veterans Affairs Organizations and therefore will store or transmit information about approximately 30,000,000 individuals. The typical affected individual is a United States Military veteran or their dependent or survivor.

The system shares transmitted information internally with a variety of VA systems including Veterans Benefit Management System (VBMS) to communicate with individuals about benefits; Veterans Health Information System Technology Architecture (VistA) imaging system to manage and communicate Electronic Health Records to VAMCs, CBOCs, and other healthcare providers, healthcare billing agencies and clearinghouses, benefit examination doctors, and pharmacies.

ECFax also shares or transmits information with a variety of other systems including those utilized by Veterans Services Organizations; contractors and vendors; American Red Cross and other blood suppliers; learning institutions including colleges, universities and trade schools; local, state, Federal and Tribal government agencies; attorneys; state and Federal prisons; and the general public. The purpose of sharing this information is to manage and execute all required communication regarding a veteran's benefits, status, and other relevant information managed by VA regarding a veteran or their dependents and survivors, as required or allowed by regulation or legislation.

As noted above all fax documentation data transmitted or received by the system is all electronic data that is protected by government approved encryption both in transit and at rest. Due to the broad nature of the types of data being transmitted a full list of interfaces is not practical. However, the list below provides a good overview of the various types and uses of the faxed data.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration Veterans Benefit Management System (VBMS) or other system dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Veterans Health Administration Veterans Health Information Systems & Technology Architecture (VistA)/Cerner or other system dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Inspector General	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers	Faxed documents and Application Programming Interface (API) as needed for

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers	specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Board of Veterans Approvals Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of General Counsel Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Office of Acquisition, Logistics, and Construction Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
National Cemetery Administration Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Congressional and Legislative Affairs Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera)	Faxed documents and Application Programming Interface (API) as needed for specific delivery of

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers	faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Human Resources and Administration Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Information and Technology Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images Any other unique identifying number, characteristic, or code	
Office of Management Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address	Faxed documents and Application

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers	Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Public Affairs Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Policy and Planning Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Operations, Security, and Preparedness Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Office of Veterans Experience Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera) • Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity	Faxed documents and Application Programming Interface (API) as needed for specific delivery of faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	
Any other IT system within any VA program office or organization Dependent upon Organization requirements	Support VA mission requirements	• Name • Date of Birth • Mother's Maiden name • Personal Email address • Personal Mailing address • Personal Phone Numbers • Emergency contact information (Name, Phone Number, et cetera)	Faxed documents and Application Programming Interface (API) as needed for specific delivery of

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Financial Account Information • Geographic Subdivisions smaller than a state • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health Plan Beneficiary Account numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • IP Address number • Device identifiers • Biometric identifiers	faxed information

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code	

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: The privacy risk of internal sharing and disclosure of data in the system is moderate. As noted in section 3.1-3.4 the system automatically deletes both transmitted fax data and fax data that in unsuccessful. The only data retained is the call detail metadata for administrative purposes as noted. However, once the data has been provided to the end user of the transmission the risk of inadvertent sharing of data is possible.

Mitigation: The ECFax system does not share information internally. Information is transmitted by users in the course of duties assigned, who have a need to know and are responsible for protecting the source and sending to the correct destination and protecting that information using applicable local procedures

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 With which external organizations (outside VA) is information shared/received? What information is shared/received, 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.

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 External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Local, State, Federal, Tribal government agencies	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Health Care Providers	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	Covered entity under HIPAA	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Benefit Examination Doctors	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	Covered entity under HIPAA	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Attorneys	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
State and Federal prisons	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor) both inbound

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		and outbound d
General Public	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Veterans and Dependents and Survivors	5 U.S. Code § 301; 44 U.S. Code § 3101	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Health Care Billing and Clearing houses	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	Covered entity under HIPAA	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Ambulance/transportation services	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Pharmacies	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	BAA, National ISA/MOU, or N/A	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Colleges, Universities, Trade, and other schools	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	5 U.S. Code § 301; 44 U.S. Code § 3101	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Veterans Service Organizations	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	National ISA/MOU as applicable, or N/A	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
Contractors/Vendors	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	BAA, National ISA/MOU, as applicable	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound
American Red Cross and other blood suppliers	Support VA mission requirements	• Names • Mother's Maiden name • Emergency contact information (Name, Phone Number, et cetera) • Geographic Subdivisions smaller than a state • Personal email address • All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death, all ages over 89 and	BAA, National ISA/MOU as applicable	Fax Transmission Any faxing data that is processed by the system is encrypted both in transit and at rest with FIPS 140-2 (or its successor)

		all elements of dates indicative of such age • Telephone numbers • Fax numbers • Social security numbers • Race/Ethnicity • Gender • Integration Control number • Military History/Service Connection • Next of Kin • Medical records numbers • Current Medications • Previous Medical Records • Health plan beneficiary numbers • Account numbers • Tax Identification Number • Certificate/License numbers • Vehicle identifiers and serial numbers including license plate numbers • Device identifiers and serial numbers • Web URLs • IP Address number • Biometric identifiers • Full face photographic images and comparable images • Any other unique identifying number, characteristic, or code		both inbound and outbound

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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.
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 privacy risk of external sharing and disclosure of data in the system is moderate. As noted in section 3.1-3.4 the system automatically deletes both transmitted fax data and fax data that in unsuccessful. The only data retained is the call detail metadata for administrative purposes as noted. However, once the data has been provided to the end user of the transmission the risk of inadvertent sharing of data is possible. All faxed data processed and transmitted by the service is expected to in service of the VAs mission to provide care and benefits as well as conduct department business functions.

Mitigation: The ECFax system does not share information externally. Information is transmitted by users who are responsible for protecting the source and sending to the correct destination and protecting that information using applicable local and organization procedures.

System audit logs will be reviewed on a periodic basis to look for errors and other issues that may impact the system as well as any potential connections to other organizations.

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? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

If the VA transmits faxed information via this service general privacy policies apply as noted in the VAs posted privacy policy on web page collection at https://www.va.gov/privacy-policy/ and https://www.va.gov/Privacy/. In addition, VA users are required to use appropriate privacy cover sheets when transmitting faxes to external and internal organizations to include all HIPAA and Privacy Act requirements. If the external users transmit faxes to the VA they must either use any organization procedures that apply or at a minimum a cover sheet detailing the recipients phone number, name (individual or office and purpose). In addition, if a VA standard form is submitted to the VA via this service the form itself will provide additional use of data and privacy information to the individual completing the form. Public notice is also published in the SORN, 90VA194 Call Detail Records – VA., and this document is published on the VA website open to anyone to read and download.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

General privacy policies are posted at https://www.va.gov/privacy-policy/ and https://www.va.gov/Privacy/ SORN is documented at https://www.govinfo.gov/content/pkg/FR-2009-04-14/pdf/E9-8448.pdf

6.1c 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.

General privacy policies are posted at https://www.va.gov/privacy-policy/ and https://www.va.gov/Privacy/ SORN is documented at https://www.govinfo.gov/content/pkg/FR-2009-04-14/pdf/E9-8448.pdf

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.

Use of the ECFax service by any party internal or external constitutes the authority to collect and transmit the faxed data. No penalty or denial of service is required.

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.

Use of the ECFax service by any party internal or external constitutes the authority to process and the consent to use of the transmitted faxed data. Use of the service is considered consent to collection, processing, and transmission of the data contained in the faxed documents

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> 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?
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: The overall privacy risks associated with notice is low. Use of the ECFax service is a user or staff requirement to complete a specific VA mission function. Transmission of faxed documents via this service constitutes an understanding and notice of consent to use the service. Notice is further supplied by SORN published in the federal registry and this PIA, which is posted on a VA public website.

Mitigation: If the VA transmits faxed information via this service general privacy policies apply as noted in the VAs posted privacy policy on web page collection at https://www.va.gov/privacy-policy/ and https://www.va.gov/Privacy/

In addition, VA users are required to use appropriate privacy cover sheets when transmitting faxes to external and internal organizations to include all HIPAA and Privacy Act requirements.

Also, if a VA standard form is submitted to the VA via this service the form itself will provide additional use of data and privacy information to the individual completing the form.

Finally, internal VA users will be provided banners and other content as reminders about use and privacy requirements of the service.

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?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The only information explicitly collected regarding individuals in the ECFax system is the information about authorized users of the system. While non-user individuals may have data about them contained within one or more faxes sent or received by the system, there is no means to identify the data in these faxes and no mechanism for users to request or access this data.

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 system is not exempt from the access provisions of the Privacy Act.

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.

Requests for audit logs and call detail records may be obtained VA standard FOIA request procedures.

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.

The only information explicitly collected about individuals by the ECFax system is to identify authorized users of the system. If user information is incorrect, a request to correct this information should be submitted to the system administrator via the helpdesk system for the administrator to correct the information. As the system only retains audit logs and call detail metadata there are no means for correcting inaccurate or erroneous information.

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.

As the system only retains audit logs and call detail metadata there are no means for correcting inaccurate or erroneous information and no means to notify users of methods of correcting their information. Standard Freedom of Information requests may be made by individuals to request available call detail records of a faxed transmission. However, details are limited to the records as noted in this PIA.

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.

As the system only retains audit logs and call detail metadata there are no means for correcting inaccurate or erroneous information and no means to notify users of methods of correcting their information hence no means to redress

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: The overall privacy risks associated with access, redress, and correction is low. Use of the ECFax service is a user or staff requirement to complete a specific VA mission function. Transmission of faxed documents via this service constitutes an understanding and notice of consent to use the service.

As the system only retains audit logs and call detail metadata there is limited ability to access, redress or and no ability to correct information in the system by these records as they are fixed administrative functions of the system.

A limited ability to search audit logs and call detail records will be available but will primarily be used for administrative purposes (billing, service level measurements, etc.)

Inherently, once the information is received by the intended destination it is the responsibility of the user to properly maintain the security of the received document.

Mitigation:

As the system only retains audit logs and call detail metadata there are very limited means to determine if a faxed document was transmitted/received with the level of details available as noted in this PIA.

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?

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.

A system administrator must create either a new account or a new user for an existing account for a user to be able to access the ECFax system.

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.

Users fall into one of three roles in general: System Administrators, who are responsible for creating new accounts in the ECFax system and/or configuring existing accounts in the system; Account Administrators, who have full access to account configuration and all account features, including the ability to add, remove, edit, activate, and deactivate users and phone numbers in the system; and General Users, who can view and send faxes, and have a limited ability to control their account configuration.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on 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. 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.

As this service is a SaaS product as defined in the PIA the support contractor will have access to and maintain all system components and the ability to see into its functionally as part of sustainment responsibilities. All contractors that support and maintain this service will be appropriately cleared to access the system. The contractor will also be required to have a Business Associate Agreement (BAA) with the VA. VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role.

Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access

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.

The VA has developed security and privacy awareness training for all valid user that have VA network access (including managers, senior executives, and contractors) that must be completed on an annual basis. System personnel certify acceptance of security and privacy responsibilities each time they access the service by signing the ECFax Rules of Behavior. In addition, the Contractor shall provide users of the system specific training on the safe and secure use of the service to include security, privacy, and rules of behavior. All VA users and VA contractors are required to complete VA Privacy and Information Security training and sign the Rules of Behavior prior to gaining access to VA data or systems.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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.***

1. The Security Plan Status, Final Draft, Accepted

2. The Security Plan Status Date, 10/18/2022

3. The Authorization Status, Authorized

4. The Authorization Date, 09/08/2022

5. The Authorization Termination Date, 09/09/2023

6. The Risk Review Completion Date, 8/18/2022

7. The FIPS 199 classification of the system HIGH

IOC Projected date 3/31/2023

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.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

This service is a commercial Software as a Service (SaaS) hosted in a AWS GovCloud environment. It does not yet have FedRAMP Authorization and is currently in the process of obtaining a VA Sponsored FedRAMP Authorization.

9.2 Does the contract with the 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 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Contract VA110-16-D-1001B3 (1) expressly limits the Contract/Subcontractor's rights to use data as described in Rights in Data – General, FAR 52.227-14(d)(1).

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.

The ECFax system collects metadata about faxes transmitted and received in order to provider Call Detail Records (CDRs) used for billing and usage reporting. Security audit logs are used for administrative purposes

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.

Overall, protection of privacy data is the responsibility of VA. Privacy and data protections policies are documented in the approved VA and Consensus security policies. These protections are also included in the contracts between VA and Consensus as well as subcontracts managed by Consensus Vendor Management team with oversight and reviewed by the CISO. All Consensus operations (cloud) receive a full risk assessment annually, which is updated and reassessed quarterly. Any deficiency is remediated and overseen by the CISO.

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).

N/A. RPA is not utilized in the ECFax information system.

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**

ID	Privacy Controls
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 they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.07.10 09:44:31 -04'00'

Privacy Officer, Tonya Facemire

SCOTT MILLER

Digitally signed by SCOTT MILLER
Date: 2023.07.07 07:26:24 -04'00'

Information System Security Officer, Scott Miller

FRANK JOY

Digitally signed by FRANK JOY
Date: 2023.07.07 11:52:24 -05'00'

Information System Owner, Frank Joy, Jr.

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).

If the VA transmits faxed information via this service general privacy policies apply as noted in the VAs posted privacy policy on web page collection at https://www.va.gov/privacy-policy/ and https://www.va.gov/Privacy/.

In addition, VA users are required to use appropriate privacy cover sheets when transmitting faxes to external and internal organizations to include all HIPAA and Privacy Act requirements. The final version of this cover sheet is not yet developed and authorized but will meet all HIPAA and Privacy Act Requirements

If the external users transmit faxes to the VA they must either use any organization procedures that apply or at a minimum a cover sheet detailing the recipients phone number, name (individual or office and purpose). The final version of this cover sheet is not yet developed and authorized.
In addition, if a VA standard form is submitted to the VA via this service the form itself will provide additional use of data and privacy information to the individual completing the form. Due to the wide array of possible documents, verbiage from each standard form cannot be provided. A general assumption is made that the appropriate data and privacy information will be included on all VA standard forms.

Public notice is also published in the SORN and this document is published on the VA website open to anyone to read and download.

SORN 90VA194 Call Detail Records – VA
Link to SORN: https://www.govinfo.gov/content/pkg/FR-2009-04-14/pdf/E9-8448.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices