



Privacy Impact Assessment for the VA IT System called:

TriZetto Facets – ClaimsXM - E (ECM CXM- E)

Veterans Health Administration (VHA)

Office of Integrated Veteran Care (IVC)

eMASS ID # 1330

Date PIA submitted for review:

03/26/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.Pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Faimafili Monaghan	Faimafili.Monaghan@va.gov	270-623-8411
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

The abstract provides the simplest explanation for “what does the system do for VA?”.

TriZetto Facets -ClaimsXM, is a managed service, contracted with Signature Choice Limited Liability Company (LLC) and it is hosted at Microsoft Azure Commercial Cloud-High. Signature Choice LLC subcontracts with Signature Performance Incorporated (Inc.), Principle Choice Solutions and Signature Performance Healthcare Administrative Services LLC. The service receives community medical, dental and pharmacy claims, applies industry standard and VA specific business rules and policy to determine what, if any, payment is due to the provider. The system ingests standard medical claim data, maintains beneficiary eligibility and utilization data, and displays in or transports status and payment data to user-accessible portals and Veteran Affairs (VA) data systems."

Overview

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

1 General Description

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

The TriZetto Facets – ClaimsXM - E is a contracted system for the Veteran Health Administration (VHA) Office of Integrated Veteran Care (IVC). The TriZetto Facets – ClaimsXM - E is a Signature Performance contractor-owned system under a managed service contract to provide claims adjudication for VHA IVC. This system does not fall under the traditional regions (1-5). The VHA IVC transmits specified files via a Secure File Transfer Protocol (SFTP) server. The TriZetto Facets – ClaimsXM - E system then retrieves the files from the SFTP server for processing within the system. Files are returned to the VHA IVC by pushing files to the SFTP server and the VHA IVC retrieves those files. Additionally, TriZetto Facets – ClaimsXM - E receives healthcare claims from VA’s Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (Civilian Health and Medical Program of the Department of Veteran’s Affairs (CHAMPVA), Spina Bifida (SB), Children of Women Vietnam Veterans (CWVV)). TriZetto Facets – ClaimsXM - E transfers payment instructions to VA’s financial management systems using file transfer. The components of the information system (servers) collecting/storing PII are Microsoft Azure Government Cloud Service – VM dynamic and AWS Microsoft Azure Government Cloud Service. The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of Health Insurance Portability and Accountability Act (HIPAA) and other Federal Regulatory information for the health care industry.

The VHA IVC supports critical services provided to Veterans and their family members by community health care providers. These services, in some cases, augment VA health care services and in others, are the sole source of health care services for the respective beneficiary population. Programs include Veteran community- based health care, Veteran Community Care Networks, CHAMPVA, SB, Camp Lejeune Family Member Program, CWVV, and Foreign Medical Program.

Accurate and timely health care claims processing services across these programs is critical to meet VA's Strategic Priorities, Veteran and family member service levels and assure appropriate use of government funds. VA seeks to have Signature Choice (prime contractor) [through its subcontractor, Signature Performance, Inc.] provide claims processing services for the CHAMPVA Program. Through use of these services, the government will improve overall process cycle times as well as accuracy with auto-adjudication of claims based on government provided business rules, regulations and policies.

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

Signature Performance owns and operates Trizetto ClaimsXM – E.

2. Information Collection and Sharing

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

Expected number of individual records is in between 500,000- 600,000. The typical client are family members of eligible veterans receiving Veteran Affairs (VA) benefits. This system falls under VA OIT Enterprise Program Management Office Cloud. There is potential that some of the records of the veteran family members and veterans also qualify under additional demographic categories. There is no way for us to know this as we do not receive data from VA that identifies them as such. Therefore, Signature will only indicate whose information will deliberately be collected for the intended purpose of the services being provided, which are "Veterans or Dependents" and "Members of the Public/Individuals."

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input type="checkbox"/>	VA Employees
<input type="checkbox"/>	Clinical Trainees
<input type="checkbox"/>	VA Contractors
<input checked="" type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

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

Veterans and Beneficiary claims data elements. To improve overall process cycle times as well as accuracy with auto-adjudication of claims based on government provided business rules, regulations and policies.

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

AWS Government Cloud Service / VM Dynamic - Tool supporting claims processing. AWS Government Cloud Service – S3 Bucket – Tool supporting claims processing. TriZetto Facets Insights – TriZetto Facets Database – TriZetto Facets is the claims processing database tool supporting claims processing adjudication services.

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

The modules/subsystems are applicable at all times.

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

ClaimsXM employs Azure Site Recovery, which is a built-in feature in Azure. All the machines are set to replicate to another region. The ClaimsXM primary region is Arizona (AZ), and the secondary region is Texas (TX). The primary machines have disk replication in place. The ClaimsXM system is configured to automatically fall over to the alternate site. Alternate storage sites are established

Version date: October 1, 2024

Page 4 of 66

by way of Azure's multiple geographic regions and across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. In the case of failure, automated processes move customer data traffic away from the affected area. The alternate storage sites are operated by Azure therefore, they have the same information security safeguards as that of the primary site

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

H. What is the citation of the legal authority?

Legal Authorities

Title 5, U.S. Code § 55 - PAY ADMINISTRATION

Title 5 U.S. Code § 301 - Departmental regulations Title 5 U.S. Code § 306 -

Agency Strategic Plans Title 26 U.S. Code § 61 - Gross income defined

Title 28, U.S. Code - JUDICIARY AND JUDICIAL PROCEDURE

Title 31 U.S. Code § 3101 - Public debt limit Title 31 U.S. Code §

3102. - Bonds

Title 31, U.S. Code § 37 - Claims

Title 38 U.S. Code § Section 31 - Foreign Medical Program

Title 38, United States Code, chapter 53 - . SPECIAL PROVISIONS RELATING TO BENEFITS

Title 38 U.S. Code § 109 - Benefits for discharged members of allied forces Title 38 U.S. Code § 111 - Payments or allowances for beneficiary travel Title 38 U.S. Code § 304 - Deputy Secretary of Veterans Affairs

Title 38 U.S. Code § 501 - VETERANS' BENEFITS Rules and regulations, 501(a), 501(b),

Title 38 U.S. Code § 527 - Evaluation and Data Collection

Title 38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation

Title 38 U.S. Code § 1703 - Contracts for hospital care and medical services in non- Department facilities

Title 38 U.S. Code § 1705 - Management of health care: patient enrollment system Title 38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care Title 38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines,

Title 38 U.S. Code § 1717 - Home health services; invalid lifts and other devices, Title 38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care Title 38 U.S. Code § 1720G - Assistance and support services for caregivers

Title 38 U.S.C. § 1721 - POWER TO MAKE RULES AND REGULATIONS

Title 38 U.S.C. § 1722 - Determination of inability to defray necessary expenses; income thresholds

Title 38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad

Title 38 U.S. Code § 1725 - Reimbursement for emergency treatment Title 38 U.S.C. § 1727 - PERSONS ELIGIBLE UNDER PRIOR LAW

Title 38 U.S. Code § 1728 - Reimbursement of certain medical expenses Title 38 U.S.C. 1741-1743. Per Diem Grant- State Home

Title 38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans,

Title 38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care

Title 38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina,

Title 38 U.S. Code § 1802 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA Sec. 1802 - Spina bifida conditions covered

Title 38 U.S. Code § Sec. 1803 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA -Healthcare

Title 38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects

Title 38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects-Health Care,

Title 38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida

Title 38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program

Title 38 U.S. Code § 5317 - Use of income information from other agencies: notice and verification

Title 38 U.S. Code § 5701 - Confidential nature of claims (b)(6)(g)(2)(g)(4)(c)(1), Title 38 U.S. Code § 5724 - Provision of credit protection and other services, Title 38 U.S. Code § 7105 - Filing of notice of disagreement and appeal,

Title 38, United States Code, section 7301(a). Functions of Veterans Health Administration: in general

Title 38 U.S. Code § 7332 - Confidentiality of certain medical records Title 38 U.S.C. 8131-8137. Construction Grant- State Home.

Title 38 Code of Federal Regulations 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).

Title 44 U.S. Code - PUBLIC PRINTING AND DOCUMENTS Veterans Access, Choice, and Accountability Act of 2014

Title 45 U.S. Code - Veterans Access, Choice, and Accountability Act of 2014.

Title 45 CFR Public Welfare Subtitle A—DEPARTMENT OF HEALTH AND HUMAN SERVICES part 160 - GENERAL ADMINISTRATIVE REQUIREMENTS.

Title 45 CFR Public Welfare Subtitle A—DEPARTMENT OF HEALTH AND

HUMAN SERVICES part 164 - SECURITY AND PRIVACY
Public Law 103–446, section 107 Veterans Education and Benefits
Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities.
Public Law 111–163 section 101. CAREGIVERS AND VETERANS’ OMNIBUS
HEALTH SERVICES ACT OF 2010- Sec. 101. Assistance and support services for
caregivers.

I. What is the SORN?

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

SORN: 24VA10A7, *Patient Medical Records - VA Care (Fee) Records* - VA (10-02-
2020), <https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

SORN: 43VA008, *Veterans, Dependents of Veterans, and VA Beneficiary Survey
Records* - VA (1-25-2021), <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf>

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health
Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf>

SORN: 79VA10, *Veterans Health Information Systems and Technology Architecture
(VistA) Records* - VA (12-23-2020), <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

SORN: 88VA244, *Centralized Accounts Receivable System/Centralized Accounts
Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* - VA
(8-13-2018), <https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf>

SORN: 147VA10, *Enrollment and Eligibility Records* - VA (8-17-2021),
<https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf>

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

No, system will not require amendment of revision of current SORNS

4. System Changes

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

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (II), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (<https://vaww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

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

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Personal Email Address | Address Numbers |
| <input checked="" type="checkbox"/> Full Social Security Number | <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a Different Individual) | <input checked="" type="checkbox"/> Medications |
| <input type="checkbox"/> Partial Social Security Number | <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Medical Records |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Race/Ethnicity |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Certificate/License Numbers | <input checked="" type="checkbox"/> Tax Identification Number |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Vehicle License Plate Number | <input checked="" type="checkbox"/> Medical Record Number |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input checked="" type="checkbox"/> Internet Protocol (IP) | <input checked="" type="checkbox"/> Sex |
| <input type="checkbox"/> Personal Fax Number | | <input type="checkbox"/> Integrated Control Number (ICN) |
| | | <input type="checkbox"/> Military History/Service Connection |
| | | <input type="checkbox"/> Next of Kin |

Version date: October 1, 2024

Page 8 of 66

- ☒ Date of Death
 ☒ Other Data Elements
☐ Business Email Address (List Below)
☐ Electronic Data
 Interchange Personal Identifier (EDIPI)

Other PII/PHI data elements: Alternative Address Information, Alternative Contact Information, Appeals and grievances information, Billed Amounts, CARC Codes, Coded Billing Information (Claim Index), Check Numbers, Coordination of Benefit Information, Current Procedural Terminology (CPT) Codes, Dental Procedure Codes, Electronic Funds Transfer Identification Numbers, FMS Document Identification Numbers, Geographical cost index codes, Geographic cost index codes, Health Insurance Numbers (Policy Number), ICD Codes, International Code Designator (ICD) Codes, Medicare Number (MBI/ HICN), Member Health Identification Numbers, National Drug Codes (NDC), Other Health Information, Paid Amounts, Patient Control Number, Personal Zip, Pharmacy/Drug Codes, Plan Names, RARC Codes, Subscriber Identification Numbers, CAGC Codes, Appeals and grievances information, Coordination of Benefits information.

1.2 List the sources of the information in the system

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

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

Source	Information
Office of Integrated Veteran Care (IVC)	The system received HIPAA standard and proprietary data transmission from IVC (VA)
TriZetto Facets ClaimsXM (subject system)	The system itself stores the information listed above
Optum Insights PPS (system)	The system received clinical and administrative coding edit information as well as payment information from Optum Insights PPS
Wolters Kluwer (entity)	Drug Data: Through their Medi-Span suite, Wolters Kluwer offers comprehensive drug data, including adverse drug effects, drug dosing and administration, drug interactions, and pricing information. This data is essential for medication-related decision-making and is available in various formats such as flat files, APIs, and web services
Telephone Calls from patient (individual)	Patient information, claims processing data and appeals and grievances information.

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.

Source	Reason for Using Information
IVC	Acts as the primary information source, ensuring the integrity and accuracy of Personally Identifiable Information (PII) and Protected Health Information (PHI).
TriZetto Facets ClaimsXM	Provides detailed claims management and processing information crucial for benefit administration and verification.
Optum Insights PPS	Enhances data quality through additional validation from external commercial data sources.
Wolters Kluwer	Supplies supplementary data to improve the overall quality and reliability of collected information.

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

Yes, the system does create information, such as analyses and reports. When such information is generated, the system itself is listed as the source of the information.

Information Source	Type of Information Created
IVC	Personally Identifiable Information (PII) and Protected Health Information (PHI)
TriZetto Facets ClaimsXM	Detailed claims management, processing, information, and claims payment information.
Optum Insights PPS	Product pricing information.
Wolters Kluwer	Product pricing information.

1.3 Methods of information collection

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

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The VHA IVC, Optum Insights PPS, and Wolters Kluwer transmit specified files via a SFTP server. The TriZetto Facets - ClaimsXM system retrieves the files from the SFTP server for processing within the system. Files are returned to the VHA IVC by pushing files to the SFTP server and the VHA IVC pulling those files down. Additionally, TriZetto Facets -

Version date: October 1, 2024

Page 10 of 66

ClaimsXM receives healthcare claims from VA's Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (CHAMPVA, SB, CWVV). TriZetto Facets - ClaimsXM transfers payment instructions to VA's financial management systems using file transfer from both Commercial aggregator and individuals.

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

Not Applicable. The information is not collected on a form.

1.4 Information checks for accuracy, and how often will it be checked.

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

To ensure the accuracy of the information processed by the TriZetto Facets – ClaimsXM - E system, the following measures are implemented:

- **Data Validation:** All incoming data undergoes rigorous validation checks daily to ensure it meets predefined standards and formats. This includes verifying the completeness and correctness of data elements such as patient names, Social Security Numbers (SSNs), dates of birth, and other personal identifiers.
- **Automated Rules and Policies:** The system applies industry-standard and VA-specific business rules and policies to automatically adjudicate claims. These rules are reviewed and updated quarterly to reflect the latest regulations and guidelines, ensuring that the claims processing is accurate and compliant.
- **Quality Assurance:** A dedicated quality assurance team conducts periodic reviews and audits of the processed data weekly. This includes cross-checking a sample of claims against source documents to verify the accuracy of the adjudication process.
- **Error Reporting and Correction:** Any discrepancies or errors identified during the validation or quality assurance processes are logged and reported immediately. The system includes mechanisms for correcting these errors promptly to maintain the integrity of the data.
- **Continuous Monitoring:** The system is continuously monitored for any anomalies or irregularities in data processing. Automated alerts are generated for any deviations from expected patterns, allowing for immediate investigation and resolution.

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

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

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

SORN: 24VA10A7, *Patient Medical Records* - VA *Care (Fee) Records* - VA (10-02-2020),
<https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

SORN: 43VA008, *Veterans, Dependents of Veterans, and VA Beneficiary Survey Records* - VA (1-25-2021), <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf>

Legal Authority: Title 5, United States Code 306; Title 38 , United States Code 527.

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf>

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

SORN: 79VA10, *Veterans Health Information Systems and Technology Architecture (VistA) Records* - VA (12-23-2020), <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

Version date: October 1, 2024

Legal Authority: Title 38, United States Code, section 7301(a).

SORN: 88VA244, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* - VA (8-13-2018),
<https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf>

Legal Authority: Title 38, United States Code, section 7301(a).

SORN: 147VA10, *Enrollment and Eligibility Records* - VA (8-17-2021),
<https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf>

Legal Authority: Title 38, United States Code, 5106.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*

This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

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

Mitigation: The ClaimsXM system is FedRAMP Authorized. All data collected, processed, and retained will be protected in accordance with NIST 800-53 moderate controls, VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Alternate Address Information	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Alternative Contact Information	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Appeals and Grievance Information	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Billed Amounts	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries,	Claims processing, Data Transmission

	audit, provide clinical insights.	
CARC Codes	Positively identify adjudication and payment information.	Claims processing, Data Transmission
CAGC Codes	Positively identify adjudication and payment information.	Claims processing, Data Transmission
Check Numbers	Positively identify payment information related to beneficiary claims.	Claims processing, Data Transmission
Coded Billing Information (Claim Index)	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information.	Claims processing, Data Transmission
Coordination of Benefit Information	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Current Procedural Terminology (CPT) Codes	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Date of Birth (DOB)	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to	Claims processing, Data Transmission

	customer service inquiries, audit, provide clinical insights.	
Date of Death (DOD)	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Dental Procedure Codes	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Electronic Funds Transfer Identification Numbers	Positively identify payment information related to beneficiary claims.	Claims processing, Data Transmission
Emergency Contact Info	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
FMS Document Identification Numbers	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries,	Claims processing, Data Transmission

	audit, provide clinical insights.	
Financial Information	Positively identify payment information related to beneficiary claims.	Claims processing, Data Transmission
Sex	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Geographic Cost Index Codes	Positively identify payment rates.	Claims processing, Data Transmission
Health Insurance Beneficiary Numbers Account numbers	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Health Insurance Numbers (Policy Number)	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
International Code Designator (ICD) Codes	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Internet Protocol (IP) Addresses	Positively identify the beneficiary, process and	Claims processing, Data Transmission

	associate claims to a beneficiary.	
Medical Record Number	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Medical Records	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Medical Records Identification Numbers	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Medications	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Medicare Number (MBI, HICN)	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Member Health Identification Numbers	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status,	Claims processing, Data Transmission

	adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	
National Drug Codes (NDC)	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Other Health Information	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Paid Amounts	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Patient Control Number	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Patient Name	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status,	Claims processing, Data Transmission

	adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	
Personal Email Address	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Personal Mailing Address	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Personal Mailing Zip	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Personal Phone	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Pharmacy/Drug Codes	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Plan Names	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
RARC Codes	Positively identify adjudication and payment information.	Claims processing, Data Transmission
Social Security Number (SSN)	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission

Subscriber Identification Numbers	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Tax Identification Number (TIN)	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit, provide clinical insights.	Claims processing, Data Transmission
Medicare Number	Positively identify the beneficiary, process and associate claims to a beneficiary. Assigned to Medicare beneficiaries and is used to track their healthcare claims and benefits. It ensures accurate processing and payment of claims under the Medicare program	Claims processing, Data Transmission
Health Insurance Beneficiary Number Account Number	Positively identify the beneficiary, process and associate claims to a beneficiary.	Claims processing, Data Transmission
Dental Procedure Codes	These codes, governed by the American Dental Association (ADA), standardize the documentation and billing for dental procedures. They facilitate efficient communication between dentists, insurance companies, and patients, ensuring accurate billing and timely insurance reimbursements.	Claims processing, Data Transmission
Coordination of Benefits Information	COB allows health plans to determine their respective payment responsibilities when an individual is covered	Claims processing, Data Transmission

	by more than one plan. It ensures that claims are paid correctly by identifying the primary payer and coordinating the payment process to avoid duplicate payments.	
FMS Document Identification Number	Positively identify the beneficiary, associate claims to a beneficiary, identify and communicate claim status, adjudication and payment information, automate workflows, respond to customer service inquiries, audit.	Claims processing, Data Transmission
Geographical Cost Index Codes	Positively identify the location services were rendered for the purposes of calculating reimbursement rates	Claims processing, Data Transmission
Appeals and Grievance Information	This data element includes details about any appeals or grievances filed by patients regarding their healthcare services or claims. It ensures that patients have a formal process to dispute decisions made by their health plans, such as claim denials or coverage issues. This information helps in tracking and resolving patient complaints, improving overall patient satisfaction and ensuring compliance with regulatory requirements.	Claims processing, Data Transmission

2.2 Describe the types of tools used to analyze data and what type of data may be produced.

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

1. **Descriptive Analytics:** *This type of analysis focuses on summarizing historical data to understand past events, such as claims and denials. By analyzing this data, patterns and trends are identified, which help*

pinpoint areas needing improvement. For example, it might reveal frequent reasons for claim denials, enabling targeted interventions.

2. **Diagnostic Analytics:** This analysis goes a step further to understand why certain events occurred. It provides detailed insights into the root causes of issues like claim denials and reimbursement delays. By diagnosing these problems, healthcare providers can implement corrective measures to prevent future occurrences.
3. **Predictive Analytics:** Utilizing historical transactional claims data, predictive analytics forecasts future outcomes at both patient and population levels. This analysis generates predictions about future claims, financial performance, and provides insights for care coordination, utilization review, and personalized treatment plans. For instance, it can predict which patients are at higher risk of hospitalization, allowing for proactive care management.
4. **Prescriptive Analytics:** Building on predictive analytics, prescriptive analytics offers recommendations on actions to take. It provides actionable insights and suggests improvements for optimizing processes like claims submission. For example, it might recommend changes in billing practices to reduce claim denials and expedite reimbursements.
5. **Discovery Analytics:** This type of analysis uncovers new insights and patterns in data that were not previously known. It reveals hidden trends and opportunities for improvement, enabling healthcare organizations to innovate and enhance their services. For instance, it might identify previously unnoticed correlations between patient demographics and claim outcomes, leading to more tailored healthcare strategies.

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?

ClaimsXM performs several types of data analysis to improve efficiency, reduce errors, and enhance financial performance:

Type of Analysis	Description	Data Created
Descriptive Analytics	Summarizes historical data to understand past events, such as claims and denials	Patterns and trends that help identify areas needing improvement
Diagnostic Analytics	Helps understand why certain events occurred	Detailed insights into the root causes of issues like claim denials and reimbursement delays
Predictive Analytics	Uses historical transactional claims data for patient-level and population-level queries to forecast future outcomes	Predictions about future claims, financial performance, and insights for care coordination, utilization review, and personalized treatment plans.

Prescriptive Analytics	Provides recommendations on actions to take based on predictive analytics	Actionable insights and suggested improvements for optimizing processes like claims submission
Discovery Analytics	Uncovers new insights and patterns in data that were not previously known	Hidden trends and opportunities for improvement

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.

When systems create or make available new information about an individual, the handling of this information typically involves:

- **Related to Existing Records:** The new information may be related to the individual's existing record to provide a more comprehensive view.
- **Creating New Records:** In some cases, a new record may be created to store the newly derived information separately.
- **Actions Based on New Data:** Actions may be taken based on the new information, such as relating an individual's profile, triggering alerts, or making decisions.
- **Access by Government Employees:** If the new information is accessible to government employees, it will be used under specific circumstances and by authorized personnel only

Analysis Type	New Records Created	Potential Actions	Roles with Access	Government Access
Descriptive Analytics	Summaries and visualizations of current and historical data	Developing dashboards and reports for stakeholder review	Business Analysts, Reporting Managers, Claims Processors, Case Managers, Healthcare Administrators, Budget Analysts, Financial Officers	Yes, Limited
Diagnostic Analytics	Identified reasons for past performance and outcomes	Analyzing root causes of historical trends and anomalies	Data Analysts, Quality Control Specialists, ITOps Team Members, Business Analysts, Code Developers	No
Predictive Analytics	Predictive data entries related to existing records	Forecasting future claims, financial performance, care coordination, utilization review, personalized treatment plans	Data Analysts, Care Coordinators, Financial Officers, Case Managers	Yes, Limited
Prescriptive Analytics	Action recommendations related to existing records	Optimizing claims submission processes	Claims Processors, Operational Managers	No
Discovery Analytics	Insights and patterns related to existing records and populations of records	Revealing hidden trends and opportunities for improvement	Data Scientists, Strategic Planners	No*

*Potential modifications to the existing contract could allow government access to discovery analytics data.

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

The information in ClaimsXM is secured through a comprehensive set of policies and procedures that cover various aspects of information security. This includes access control, awareness training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, and system and information integrity. The policy ensures the confidentiality, integrity, and availability (CIA) of Signature's information systems. The ClaimsXM system is FedRAMP authorized (moderate). All required NIST and FedRAMP 800-53 controls have been implemented.

To specifically protect data in transit and at rest, the following measures are implemented:

- **Encryption:** Data in transit is encrypted with TLS 1.2 active, ensuring secure communication channels. All data at rest is encrypted using Microsoft Azure AES 256 encryption algorithms. This ensures that even if the storage media is compromised, the data remains protected and inaccessible without the appropriate decryption keys.
- **Access Controls:** Strict access controls ensure that only authorized personnel can access sensitive data. This includes role-based access controls and regular audits to monitor access.
- **Regular Audits:** Regular security audits and assessments help identify and mitigate potential vulnerabilities, ensuring that the system remains secure and compliant with relevant security standards.

These measures collectively ensure the security and privacy of data in transit and at rest, aligning with the specified controls and regulatory requirements.

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

Yes, additional protections are in place to safeguard Social Security Numbers (SSNs). These include:

- **Masking or Truncating SSNs:** Displaying only partial SSNs to reduce exposure. This helps minimize the risk of unauthorized access to the full SSN.
- **Access Restrictions:** Strict access control measures are implemented to ensure that only authorized personnel have access to SSNs. This includes role-based access controls and regular audits to monitor access. Access to SSNs is limited to only those who need it for their job functions.
- **Multi-Factor Authentication (MFA):** MFA is required for accessing systems that handle SSNs, providing an additional layer of security.
- **Monitoring and Auditing:** Continuous monitoring and auditing of access to SSNs are conducted to detect and respond to any unauthorized access attempts.

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

Version date: October 1, 2024

The system ClaimsXM system is FedRAMP authorized. Specifically, Personally Identifiable Information (PII) and Protected Health Information (PHI) are safeguarded in accordance with OMB Memorandum M-06-15 through the following measures:

Rules of Conduct:

- Implemented NIST 800-53 PL-4 (Rules of Behavior): Establishes rules of behavior for individuals accessing the system and requires signing of our internal Rules of Behavior as well as VA's Rules of Behavior.
- Implemented NIST 800-53 AT-2 (Awareness Training): All individuals with access complete awareness training at time access is granted and at minimum, annually thereafter.

Administrative, Technical, and Physical Safeguards:

- Implemented NIST 800-53 AC-1 (Access Control Policy and Procedures): Develop and disseminate access control policies and procedures.
- Implemented NIST 800-53 SC-28 (Protection of Information at Rest): Ensure that information at rest is protected through encryption and other means.
- Implemented NIST 800-53 SC-9 (Transmission Confidentiality and Integrity): Protect data in transit through encryption and other security measures.

Privacy Official:

- Implemented NIST 800-53 PM-3 (Information Security Resources): Assign a senior official responsible for privacy and information security resources.
- Conduct Privacy Impact Assessments (PIAs):
- Implemented NIST 800-53 RA-3 (Risk Assessment): Conduct risk assessments, including privacy impact assessments, to evaluate the impact of systems on privacy.

Data Minimization:

- Implemented NIST 800-53 AC-6 (Least Privilege): Ensure that only the minimum necessary data is collected and accessed by authorized personnel.
- Implemented NIST 800-53 SI-12 (Information Handling and Retention): Implement policies for handling and retaining information to minimize data collection.

Training and Awareness:

- Implemented NIST 800-53 AT-3 (Role-Based Training): Require all individuals with access to complete role-based training (upon access being granted and at minimum, annually thereafter, on privacy and security best practices.
- Implemented NIST 800-53 AT-4 (Security Training Records): Maintain records of security and privacy training provided.

Audits and Assessments:

- Implemented NIST 800-53 CA-2 (Security Assessments): Conduct regular security assessments to identify and mitigate potential vulnerabilities.
- Implemented NIST 800-53 CA-7 (Continuous Monitoring): Implements continuous monitoring to ensure the effectiveness of security controls.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

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?

Access to PII by Signature Performance's associates is based on a need to know to perform the Associate's job function. Additionally, system access is based on Role Based Access Controls (RBAC). The RBAC model will ensure proper separation of duties in the system.

Access to the system will be requested through the IT ticketing system where the Associate's manager will need to provide approval for the system access. Once access is approved the Associates profile will be developed based on the designated RBAC model for the Associates job function. Upon termination of employment, the Associate's access to the system is removed immediately. System access is reviewed quarterly and documented in the ticketing system.

Access to the TriZetto Facets - ClaimsXM system is logged and monitored through a Security Information and Event Management (SIEM) solution managed and maintained by Signature Performance. Specifically, the following controls with associated policies and procedures have been implemented to enforce approved authorizations for access to ClaimsXM information and system resources:

- **Access Control Policies and Procedures (AC-1):** Establishes the policies and procedures for access control.
- **Account Management (AC-2):** Manages information system accounts, including establishing, activating, modifying, disabling, and removing accounts.
- **Access Enforcement (AC-3):** Enforces approved authorizations for logical access to information and system resources.
- **Information Flow Enforcement (AC-4):** Enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.
- **Separation of Duties (AC-5):** Ensures that the duties of individuals are divided to reduce the risk of malevolent activity without collusion.

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

Criteria, procedures, controls, and responsibilities are documented in the ClaimsXM SSP, SSP

attachments, Signature Performance policies and procedure documentation.

2.4c Does access require manager approval?

Yes, access to ClaimsXM requires the individual's functional manager's approval in addition to the System Administrator approval.

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

Yes, access to the TriZetto Facets - ClaimsXM system is logged and monitored through a Security Information and Event Management (SIEM) solution managed and maintained by Signature Performance.

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

Signature Performance Information Security Office and the ClaimsXM admin team is responsible for assuring safeguards for the PII.

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

- *Alternate Address Information*
- *Alternative Contact Information*
- *Appeals and grievances information*
- *Billed Amounts*
- *CARC Codes*
- *CAGC Codes*
- *Check Numbers*
- *Coded Billing Information (Claim Index)*
- *Coordination of Benefit Information*
- *Coordination of Benefits Information*
- *Current Procedural Terminology (CPT) Codes*
- *Date of Birth (DOB)*
- *Date of Death (DOD)*

- *Dental Procedures Codes*
- *Electronic Fund Transfer Identification Numbers*
- *Emergency Contact Info*
- *FMS Document Identification Number*
- *Financial Information*
- *Sex*
- *Geographical cost index codes*
- *Health Insurance Beneficiary Number Account numbers*
- *Health Insurance Numbers (Policy Number)*
- *International Code Designator (ICD) Codes*
- *Internet Protocol (IP) Addresses*
- *Medicare Number (MBI/HICN)*
- *Medications*
- *Medical Records*
- *Medical Records Identification Numbers*
- *Member Health Identification Numbers*
- *National Drug Codes (NDC)*
- *Other Health Information*
- *Paid Amounts*
- *Patient Control Number*
- *Patient Name*
- *Personal Email Address*
- *Personal Mailing Address*
- *Personal Phone*
- *Personal ZIP*
- *Pharmacy/Drug Codes*
- *Plan Names*
- *RARC Codes*
- *Social Security Number (SSN)*
- *Subscriber Identification Numbers*
- *Tax Identification Number (TIN)*

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

The contractor will follow the VHA Records Retention Schedule 10-1 @ <https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf>. Sections 1260- Civilian Health and

Version date: October 1, 2024

Page 30 of 66

Medical Care Program and 4000- Financial Management and Reporting Records or 6000- Health Information Management Service (HIMS). Also, procedures under the contract, Media Sanitization Policy (OIT-OIS SOP MP-6-Electronic Media Sanitization) and Records Management Policy (VHA Directive 6300 Records Management). 1260 Care in Community, Health and Medical Care Program, VA. Compensation, Pension and Vocational Rehabilitation, Records Control Schedule 10-1, 1180 1180 Office of General Counsel; VA Central Office (VACO) and Regional Offices; 1180.17. Veterans Benefits.

Trizetto Facets ClaimsXM– Information is maintained until 3 years after final payment or a shorter period of time as specified in FAR subpart 4.7, per VA contract. ClaimsXM transfers records to VA at regularly cadences intervals and is not an official system of record. The records in ClaimsXM are considered duplicative of what VA maintains. At the end of the required storage period, the records are destroyed in adherence with applicable laws, regulations, policies and procedures.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.

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

Signature Choice - Signature's record retention policy (with enclosed schedule) was developed, reviewed and approved by legal counsel. The policy is also reviewed annually by the internal policy subcommittee.

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

Trizetto Facets ClaimsXMis not the system of record. Please see Record Control Schedule (RCS) 10–1 item (<http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>).

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

Record Control Schedule (RCS) 10 1 item (<http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>).

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

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Prior to termination or completion of this contract, Signature must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of

VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and VA Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and Media Sanitization Policy (OIT-OIS SOP MP-6-Electronic Media Sanitization), Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), <https://www.va.gov/vapubs>. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), <https://www.va.gov/vapubs>. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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 allow this, and third-party service providers are not permitted to do so either. All testing data is de-identified prior to transference, use, and testing.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by TriZetto Facets ClaimsXM – E could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, TriZetto Facets ClaimsXM – E adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual’s information is carefully disposed of by the determined method as described in the records control schedule.

Signature has an internal records administrator process overseen by corporate compliance. Each department undergoes monthly reviews of records that either meet the expiration date or will meet the expiration date prior to the next scheduled review. Each designated department record administrator reviews the records in questions with corporate compliance, follow the proper process for record destruction and provide notification to compliance of the destruction.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a ClaimsXM consists of 1 key component (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ClaimsXM and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
TriZetto Facets – ClaimsXM Database	Yes	Yes	<ul style="list-style-type: none"> • <i>Patient Name</i> • <i>Social Security Number (SSN)</i> • <i>Date of Birth (DOB)</i> • <i>Date of Death (DOD)</i> • <i>Personal Mailing Address</i> • <i>Personal ZIP</i> • <i>Personal Phone</i> • <i>Personal Email Address</i> • <i>Sex,</i> • <i>Emergency Contact Info</i> • <i>Health Insurance Beneficiary Number Account numbers</i> • <i>Health Insurance Numbers (Policy Number)</i> • <i>Medications</i> • <i>Medical Records</i> • <i>Medical Records Identification Numbers</i> • <i>Tax Identification Number (TIN)</i> 	Claims Adjudication	MFA controlled access point. RBAC in place. FIPS 140-2 Encryption for data in transit. Data at rest is encrypted with SHA-256 algorithm.

			<ul style="list-style-type: none"> • <i>Subscriber Identification Numbers</i> • <i>Medicare Number (MBI/HICN)</i> • <i>Member Health Identification Numbers</i> • <i>Plan Names</i> • <i>Current Procedural Terminology (CPT) Codes</i> • <i>International Code Designator (ICD) Codes</i> • <i>National Drug Codes (NDC)</i> • <i>Dental Procedures Codes</i> • <i>Pharmacy/Drug Codes</i> • <i>Billed Amounts</i> • <i>Paid Amounts</i> • <i>Other Health Information</i> • <i>Coordination of Benefits Information</i> • <i>FMS Document Identification Number</i> • <i>Check Numbers</i> • <i>Electronic Fund Transfer Identification Numbers</i> • <i>Patient Control Number</i> • <i>Coded Billing Information (Claim Index)</i> • <i>Geographical cost index codes</i> • <i>CARC Codes</i> 		
--	--	--	---	--	--

			<ul style="list-style-type: none"> • <i>RARC Codes</i> • <i>CAGC Codes</i> • <i>Appeals and grievances information</i> • <i>Alternate Address Information</i> • <i>Alternative Contact Information</i> • <i>Internet Protocol (IP) Addresses</i> • <i>Financial Information</i> • <i>Coordination of Benefit Information</i> • <i>Member Health Identification Number</i> 		
--	--	--	--	--	--

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

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

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

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

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

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

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
VA Office of Information Technology Veterans Data Integration and Federation Enterprise Platform	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical	Secure File Transfer Protocol (SFTP)

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number	
VA Enterprise Cloud Amazon (AWS) Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS)	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid	SFTP

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number	
Veterans Health Administration Office of Integrated Veteran Care Claims Processing and Eligibility (CP&E)	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member	SFTP

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number	
Financial Service Center (FSC) Financial Management System	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPAA	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary	File Transfer Protocol with SSL Security

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
	and other Federal Regulatory information for the health care industry.	Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit	

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		Information, Member Health Identification Number	
VA Enterprise Cloud Microsoft Azure Program Integrity Tool (PIT)	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical	SFTP

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number	
VA Veteran Family Member (VFMP) Program Care Coordination and VFMP Clinical Quality Teams under the VFMP Integrated External Networks	The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid	<i>Secure File Transfer Protocol (SFTP) with VA PED TAS</i>

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
		Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: This is a cloud-based system where the Cloud Service Provider (CSP) Third-Party Assessment Organization (3PAO) already conducts penetration testing and defense in depth. Flaw remediation is centrally managed through four separate processes:

- The deployment of antivirus configurations to all system servers
- The use of configuration management to centrally manage the identification of all required

Windows patches and to install them on appropriate servers.

- The use of Ansible to centrally manage the identification of all required Linux patches and to install them on appropriate servers.
- Monthly Nessus scanning informs system staff of required security vulnerabilities and fixes. System staff also conduct their own monthly Nessus scans to identify and interpret system vulnerabilities. Scanning results are reported, analyzed and recorded for remediation. The information system fails to a stopped state for database integrity and disk space problems, preserving existing data and audit records in failure. Systems are backed up continuously to an alternate site. In the event of a catastrophic failure, the system can be restored from alternate site or failed over to run at the alternate site. As stated within the Azure System Security Plan, Azure will prevent the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. Data confidentiality and integrity is ensured via administrative, technical and physical controls. Physical access to the servers is restricted to authorized personnel in a data center at a facility with 24-hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 List the external organizations (outside VA) that information shared/received, and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	List the purpose of information being shared / received / transmitted	List the specific PII/PHI data elements that are processed (shared/received/transmitted)	List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data
Change Health Care Clearing House Change Health Care (Contractor)	Claims processing. Data Transmission through SFTP	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits	MOU/ISA, BAA	Business Partner Extranet (BPE)

Version date: October 1, 2024

Page 46 of 66

		Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number		
Signature Choice (Contractor) Signature Performance (Sub Contractor)	Claims processing. Data Transmission through SFTP	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check	MOU/ISA, BAA	B Business Partner Extranet (BPE) [Business Partner Extranet [BPE], firewall, and other connections) on and to a VA. Trusted Internet Connection (TIC) Gateway]

		Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number		
Globalscape (System) Change Healthcare (Contractor)	Claims processing. Data Transmission through SFTP	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers,	MOU/ISA BAA	S2S VPN Tunnel [Trusted Internet Connection (TIC) Gateway.

		Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number		
Pharmacy Benefits Manager Optum RX (Contractor)	Claims processing. Data Transmission through SFTP	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim	MOU/ISA BAA	Business Partner Extranet (BPE)

		Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number		
Signature Choice (Contractor) Principle Choice Solutions (Sub Contractor)	Claims processing. Data Transmission through SFTP	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone, Medical Record Number, Sex, Emergency Contact Info, Health Insurance Beneficiary Numbers Account numbers, Medications, Medical Records, Tax Identification Number (TIN), Subscriber ID, Medicare Number (MBI, HICN), Member Health ID, Date of Death, Plan Name, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Billed Amounts, Paid Amounts, Other Health Information, FMS Document ID	MOU/ISA BAA	Business Partner Extranet (BPE)
Signature Choice (Contractor) Signature Performance Healthcare Administrative Services LLC (Sub Contractor)	Claims processing. Data Transmission through SFTP	Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Personal Mailing Address, Personal ZIP, Personal Phone, Personal Email Address, Sex, Emergency Contact Info, Health Insurance Beneficiary Number Account numbers, Health Insurance Numbers (Policy Number), Medications, Medical Records, Medical Records	Business Partner Extranet (BPE)	ISA/MOU BAA

		Identification Numbers, Tax Identification Number (TIN), Subscriber Identification Numbers, Medicare Number (MBI/HICN), Member Health Identification Numbers, Plan Names, Current Procedural Terminology (CPT) Codes, International Code Designator (ICD) Codes, National Drug Codes (NDC), Dental Procedures Codes, Pharmacy/Drug Codes, Billed Amounts, Paid Amounts, Other Health Information, Coordination of Benefits Information, FMS Document Identification Number, Check Numbers, Electronic Fund Transfer Identification Numbers, Patient Control Number, Coded Billing Information (Claim Index), Geographical cost index codes, CARC Codes, RARC Codes, CAGC Codes, Appeals and grievances information, Alternate Address Information, Alternative Contact Information, Internet Protocol (IP) Addresses, Financial Information, Coordination of Benefit Information, Member Health Identification Number		
--	--	---	--	--

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized program, system, or individual.

Mitigation: All users with access to Trizetto Facets- Claim XM undergo Privacy and Security training (VA10176 or equivalent) and sign a Rules of Behavior. There are penalties for non-compliance with rules of behavior for VA users and contractual penalties for the vendor. Access is limited based on need to know.

All ClaimsXM users to include privileged users must authenticate via MFA. Once a user has access to the system, their access is based on their specific role (RBAC). User access is reviewed each quarter in alignment with NIST and FedRAMP requirements. User access logs are reviewed each week via the Manage Engine Event Log Analyzer. Any information shared outside of the system is covered with a Memorandum of Understanding or an Interconnection Security Agreement.

ClaimsXM is not a system of record nor is their direct access to any VA customer. Claims information is supplied to ClaimsXM system via an encrypted SFTP server.

Section 6. Notice

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

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

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

Trizetto Facets ClaimsXM- This Privacy Impact Assessment is the only form of notice, as information is not collected directly from an individual. PII/PHI is collected by a commercial non-VA provider at the point of service. Information is collected from a non-government source and sent either from the Third-Party Administrators (TPA) or directly from a non-VA provider, so there is no opt-out or explanation of government use.

SORNs

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

SORN: 24VA10A7, *Patient Medical Records - VA Care (Fee) Records* - VA (10-02-2020),
<https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf>

SORN: 43VA008, *Veterans, Dependents of Veterans, and VA Beneficiary Survey Records* - VA (1-25-2021),
<https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf>

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015),
<https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf>

SORN: 79VA10, *Veterans Health Information Systems and Technology Architecture (VistA) Records* - VA (12-23-2020), <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

SORN: 88VA244, *Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)* - VA (8-13-2018),
<https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf>

SORN: 147VA10, *Enrollment and Eligibility Records* - VA (8-17-2021),
<https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf>

6.1b If notice was not provided, explain why.

This Privacy Impact Assessment is the only form of notice, as information is not collected directly from an individual. Information is collected from a non-government source and sent either from the Third-Party Administrators (TPA) or directly from a non-VA provider, so there is no opt-out or explanation of government use.

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

This Privacy Impact Assessment is the only form of notice and is posted publicly.

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.

Trizetto Facets ClaimsXM system - PII/PHI is collected by a commercial non-VA provider at the point of service.

Information is collected from a non-government source and sent either from the Third-Party Administrators (TPA) or directly from a non-VA provider, so there is no opt-out or explanation of government use.

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.

Trizetto Facets ClaimsXM- PII/PHI is collected by a commercial non-VA provider at the point of service. Information is collected from a non-government source and sent either from the Third-Party Administrators (TPA) or directly from a non-VA provider, so there is no opt-out or explanation of government use.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: Sufficient notice has not been provided to the individual therefore the individuals are unaware that their information is being collected.

Mitigation: This system does not collect data directly. Privacy Rights are provided at the point of care and through program guides individuals are notified that their information is being collected and used. Individuals can decline to provide information, as a result services will be delayed.

Data is encrypted at rest. The System of Records Notice (SORN) and the Privacy Impact Assessment (PIA) serve as critical mitigation factors by ensuring that privacy risks are identified, assessed, and managed, thereby enhancing compliance with privacy laws and protecting sensitive data.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.

Privacy notice provided at the point of service addressed redress. Any records generated by the system will be the responsibility of the VA to maintain, retain, and act upon any applicable Freedom of Information Act, Privacy Act, or HIPAA requests. Individuals can submit a request for information through the VHA Office of Integrated Care FOIA/Privacy Office
vha.ivc.po@va.gov or vha.ivc.FOIA@va.gov.

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)?

Not Applicable. 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?

Not Applicable. The system is a Privacy Act system.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

To correct data in VHA Systems the Beneficiary will call the VHA Call center at: 1-916- 692-7450 Beneficiary Customer service telephone line: 1-800-733-8387. Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

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

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.

Beneficiary will call the VHA Call center at: 1-916-692-7450

Beneficiary Customer service telephone line: 1-800-733-8387

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will Version Date: February 27,2020 Page 32 of 38 accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:

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

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

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

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

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

Beneficiary will call the VHA Call center at: 1-916-692-7450

Beneficiary Customer service telephone line: 1-800-733-8387

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: *The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

Principle of Individual Participation: *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

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

Follow the format below:

Privacy Risk: If the VHA IVC employee enters the data incorrectly, and the veteran/beneficiary is not paid accurately.

Mitigation: The Veteran/Beneficiary or provider can contact the claims payment customer service support telephone line, Beneficiary: 1-800-733-8387 or they may contact the VHA IVC Privacy office vha.ivc.po@va.gov.

Section 8. Technical Access and Security

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

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

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

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

Access to PII by Signature Performance Associates is based on a need to know to perform the Associate's job function. Additionally, system access is based on Role Based Access Controls (RBAC). The RBAC model ensures proper separation of duties in the system. Access to the system will be requested through the IT ticketing system where the Associate's manager must provide approval for the system access.

Prior to authorizing access to the Information System, personnel are required to have favorable background investigations or have been granted interim access by the contract COR (Contracting Office Representative). Signature Choice' Human Resources (HR)/Recruiting department is responsible for ensuring any required screening of newly added associates occurs prior to access being granted. The Program Manager in coordination with HR will ensure this re-screening occurs prior to being granted access.

Once access is approved the Associates profile will be developed based on the designated RBAC model for the Associates job function. There are no users from other agencies that have access to the TriZetto Facets - ClaimsXM system.

Administrators, Domain Admins, and Service Accounts are privileged accounts; these functions are issued for use and management of applications, devices and systems and used to run services such as backups/restores. User accounts Identification are general user accounts and use data viewer/manipulation. Process identification rolls are application accounts, these include general user functions.

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?

There are no other agencies with 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.

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
Administrators	Internal	P	Moderate	Full administrative access	Issued for use and management of applications, devices and systems
Domain Admins	Internal	P	Moderate	Full administrative access	Add/remote client users. Create, modify and delete client applications

User Account IDs	Internal	NP	Limited	N/A	Data viewer/manipulation
Processor IDs	Internal	NP	Moderate	N/A	General users
Service Account	Internal	P	Limited	NA	Used to run services such as backups/restores.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

Signature Choice, LLC, is the prime contractor in support of the US Department of Veterans Affairs (VA) and its joint venture partners personnel are required to sign non-disclosure agreements (NDAs) as part of VA security clearance requirements. Contractors will have access to the system to perform claims adjudication and system administrative functions. The design and maintenance of the system is maintained and performed by Signature Performance, Inc. in accordance with its subcontract agreement with Signature Choice, LLC.

Contractors are required to sign an Rules of Behavior. A signed BAA is completed. The bridge contract number is 36C10G24D0051. The Task Order number is 36C10G24N0058.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Contractors are required to sign an Rules of Behavior. A signed BAA is completed. The bridge contract number is 36C10G24D0051. The Task Order number is 36C10G24N0058.

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

Contractors will have access to the system to perform claims adjudication and system administrative functions.

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

The design and maintenance of the system is maintained and performed by Signature Performance, Inc. in accordance with its subcontract agreement with Signature Choice, LLC.

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

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

This question is related to privacy control AR-5, Privacy Awareness and Training.

Privacy and Security Training

- Security awareness (cyber awareness) and HIPAA Security and Privacy Rule training is administered.
- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training includes but is not limited to and based on the role of the user.

- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 3867207: Information Security Role-Based Training for System Owners
- VA 3914020 Contingency Plan Role Based Training

Signature Choice provided mandatory Privacy and Security Training:

- Annual DoD Cyber Awareness Challenge for all Associates
- Technology Use at Signature for all Associates
- Associate Guidebook Review and Acknowledgement for all Associates
- HIPAA Compliance Training for all Associates
- Confidential Information Policy for all Associates
- Incident Response Training for IRT Core members – Role-based training

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

8.4a If completed, provide:

1. *The Security Plan Status:* **Completed**
2. *The System Security Plan Status Date:* **06/22/2023**
3. *The Authorization Status:* **Granted**
4. *The Authorization Date:* **11/19/2020**
5. *The Authorization Termination Date:* **11/19/2025**
6. *The Risk Review Completion Date:* **10/19/2020**
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* **Moderate**

Version date: October 1, 2024

Page **60** of **66**

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 not completed or In Process, provide your **Initial Operating Capability (IOC) date**.

A&A information provided above in section 8.4a.

Section 9 – Technology Usage

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

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

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

Trizetto Facets ClaimsXM- Yes. Microsoft Azure Government Cloud. FedRAMP approved. Package ID F1603087869.

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

All data is the intellectual property of the U.S. Department of Veterans Affairs; Vendors do not have any direct access to the government data and must maintain confidentiality under its contract terms and conditions with Signature Choice, Inc. The bridge contract number is 36C10G24D0051. The Task Order number is 36C10G24N0058.

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.

Signature's contract with the Veteran Administration explicitly states that all PHI is and remains data owned by Covered Entity (VA), as long as Business Associate creates, receives, maintains, or

transmits PHI, regardless of whether a compliant Business Associate Agreement is in place. Signature Choice is the host and responsible party for ClaimsXM, its operations, and data that resides within ClaimsXM. Microsoft Azure provides the cloud space to host ClaimsXM. However, ClaimsXM is the CSP to the direct clients.

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.

Signature Choice - Our Business Associate Agreements (BAAs) with sub-business associates include this language. Yes, security and privacy controls stipulated within contracts between SP and Covered Entities are incorporated into contractual agreements between SP and vendors.

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

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

The ClaimsXM system does not utilize Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Eller Pamintuan

Information System Security Officer, Faimafili Monaghan

Information System Owner, Dena Liston

APPENDIX A-6.1

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

[Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES](#)

[23VA10NB3, Non-VA Care \(Fee\) Records-VA - \(7-30-2015\)](#)

[24VA10A7, Patient Medical Records-VA -\(10-2-2020\)](#)

[43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA \(1-25-2021\)](#)

[54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA \(3/3/2015\)](#)

[79VA10, Veterans Health Information Systems and Technology Architecture \(VistA\) Records – VA \(12/23/2020\)](#)

[88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System \(CAR/CAROLS, combined system referred to as CAO\) - VA \(8-13-2018\)](#)

[147VA10, Enrollment and Eligibility Records - VA \(8-17-2021\)](#)

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

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

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Directive 1605.04

IB 10-163p (va.gov)