Privacy Impact Assessment for the VA IT System called:

4Cast

Veterans Health Administration
Administer Health Care Business

Date PIA submitted for review:

July 14, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Wilson, Andrea	Andrea.Wilson3@va.gov	(321) 205-4305
Information System Security Officer (ISSO)	Ross, Jeff	Jeff.Ross@va.gov	(307) 778-7343
Information System Owner	Wildes II, Larry	Larry.Wildes@va.gov	(406) 447-7673

Abstract

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

4Cast, as a Managed Service, is a resource planning tool used by medical center and VISN leadership to efficiently aggregate and prioritize the fiscal and non-monetary resource needs of individual facilities. 4Cast collects the individual business/operating plans by fiscal year for each service line within a VA medical center as documented by the Service Chief or a designated administrator. The information collected includes strategic and tactical objectives, Full Time Equivalent (FTE) employee losses and gains, equipment and space requests. Additionally, workload data is used by the Services as a basis of estimate for future resource requests. Tracking progress via monitoring reports gives administrators accurate information to ensure that actual resource utilization maps to forecast plans. Intention of this site is to help VA plan and manage expenses. Vendor website hosted on the Amazon GovCloud. No PII or PHI is allowed, and a login banner states this to all users. Access is protected by username/password separate and distinct from VA usernames and passwords.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

4Cast is a managed service provider, accessible via the internet and deployed on cloud resources for Veteran's Health Administration (VHA) hospitals. It was purposefully built as a resource planning tool used by medical center and VISN leadership to efficiently aggregate and prioritize the fiscal and non-monetary resource needs of individual facilities. 4Cast collects the individual business/operating plans by

fiscal year for each service line within a VA medical center as documented by the Service Chief or a designated administrator.

4Cast maintains approximately 3600 business plans spanning five fiscal planning years. The business plans are typically created by a Service Chief or an Administrative Officer (AO) and contain summary data for fiscal resources (Contracts and Fund Control Point (FCP) information) and personnel records. Fiscal expenditures and obligations come from the Statement of Account (SOA) from each participating facility and the personnel records come from the PAID database of VA employees. This information is mapped to the individual services within the facility by Time and Leave (T&L) codes and FCPs. The purpose of this information is to provide a current snapshot of a service's resources and a baseline to evaluate new requests (financial and personnel hires) for the upcoming fiscal year. Additional information captured by 4Cast as part of the business planning process includes a description of the service, and analysis of strengths, weaknesses, opportunities and challenges (SWOC), current and future workload expectations, current and planned goals and tactical objectives, and resource requests for Full Time Employee Equivalents (FTEE), Overtime, Fee Providers, FCPs, and planned Travel and Education expenditures. Additionally, 4Cast provides reporting capabilities of current expenditures compared to current budgets in a Monitoring function for each of the resource areas listed above.

4Cast is not a regional GSS, VistA or LAN and is available via license purchase for any VA Medical Center or VISN. Currently there are 18 VA Medical Centers with active 4Cast licenses. There are roughly 2900 active users of 4Cast.

4Cast does not share information with other IT systems.

4Cast is deployed on cloud technology and exists in a single environment (site) in the Amazon GovCloud and is accessible via the internet. Therefore, a single set of controls govern all technology and data.

4Cast has a current ATO with condition signed May 14, 2021

The completion of this PIA will not result in circumstances that require changes to business processes or technology.

4Cast does not require a SORN.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Other Unique Identifying Information (list below)

Employee Name (Stored in a masked form)
Employee ID (Stored in a converted unique identifier)

PII Mapping of Components

4Cast consists of 4 key components (WebServer, AppServer. Relational Database. Bulk File Storage). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by 4Cast and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Relational Database (Amazon RDS Server)	Yes	Yes	Employee Name, Employee ID	Identification of Full Time Equivalent resources by service area within VA	Conversion (ID) and Masking (Name)

				Hospital, and the unique identification of work hours over time by FTE	
Web Server (Apache)	No	No	N/A	N/A	N/A
Application Server (Tomcat)	No	No	N/A	N/A	N/A
User File Store (Amazon S3 Bucket)	No	No	N/A	N/A	N/A

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

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

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

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

PERSONNEL AND ACCOUNTING INTEGRATED DATA (PAID): The primary function is the collection and transmission of Time and Attendance (T&A) Report data. The purpose of this function is to provide an electronic means by which biweekly payroll data can be collected, processed, and transmitted to the Department of Veterans Affairs' Austin Automation Center (AAC) in Austin, Texas. 4Cast uses this information to track the number of FTEE assigned to each service within a facility for every pay period for planning and monitoring purposes.

HR SMART: HR Smart is VA's human resources information system that supports personnel suitability, payroll, and position management. HR Smart organizes data by position, rather than by employee, and allows for real-time human resources transaction processing for all of VA. Data pertaining to current staff, gains and losses, and vacancies are obtained from HR Smart. 4Cast obtains vacancy and position related information to track open positions for monitoring and vacant positions to minimize data entry for users creating business plans.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Both PAID and HR Smart data files are Flat File Excel submitted via email to 4Cast Support team and uploaded into 4Cast database by 4Cast Technical Team through the use of an Extract, Transform, and Load (ETL) tool.

1.4 How will the information be checked for accuracy? How often will it be checked?

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The Plan 4 Healthcare staff performs several reviews of pre-loaded data. Once the ETL process runs to import the data into the database, automated data checks and logs are reviewed by the analyst to confirm there were no issues. The support staff next reviews 4Cast online to ensure that the data is presenting correctly to the end users.

Once this internal process is complete, the medical center Fiscal staff is notified that data has been processed. For business planning purposes, any pre-loaded data is validated both by the Fiscal staff and the Service level staff as they are compiling their resource plans. This includes both financial and non-financial (FTEE) resources. If a refresh is required to update the data to current (time has passed and a new pay period of data is available), the same Fiscal Staff and Service level staff review takes place before business planning is finalized. Once business plans are submitted for management review, the plan is locked and cannot be edited.

For monitoring purposes, new data is received every two weeks when a new pay period of data is available in PAID. Once this data is loaded into 4Cast, the Fiscal staff is notified and performs a review of the data to validate it was loaded correctly.

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

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

Not Applicable: Privacy Act (e)(3) statement is not required. As documented in the System Security Categorization Report, 4Cast is a resource planning tool used by medical center and VISN leadership to efficiently aggregate and prioritize the fiscal and non-monetary resource needs of individual facilities. The information collected includes strategic and tactical objectives, Full Time Equivalent (FTE) employee losses and gains, equipment, and space requests. 4Cast does not contain sensitive information such as PII/PHI and only collects employee names (masked during data load) and employee IDs (scrambled and not stored). The use of Employee Name is stored and displayed in a masked format Last Name, First Three Letters of First Name *** (e.g. Smith,Joh***). The Employee ID is converted via an algorithm into a separate unique identifier and is only stored in the database, not displayed to the end users. The information stored and displayed in 4Cast is considered "rolodex exception" information that is publicly available. This information is not PHI or connected to any other information regarding VA employees.

4Cast has a current ATO with condition signed May 14, 2021.

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There are no privacy risks regarding the data stored in 4Cast. While it is necessary to uniquely identify individual FTEE within a facility for planning and monitoring purposes, the use of Employee Name is masked when stored and displayed in 4Cast and is considered "rolodex exception" information that is publicly available. The Employee ID is retained but is converted via an algorithm to a unique identifier. The purpose of this unique identifier is only to tie together records between pay periods for an individual employee to ensure that they are not double counted and therefore is not necessary to store the original Employee ID. This information is not PHI or connected to any other information regarding VA employees.

Mitigation: The Employee ID is stored and displayed in a masked format Last Name, First Three Letters of First Name *** (e.g. Smith,Joh***). The Employee ID is converted via an algorithm into a separate unique identifier and is only stored in the database, not displayed to the end users.

Section 2. Uses of the Information

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

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

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

4Cast collects tactical planning information and resources requests related to both operational needs and resources necessary for goal attainment for the services within a medical center facility. Additionally, the data 4Cast receives from existing VA systems is used to compare current versus budgeted information with the monitoring module within an existing fiscal year. The extent to which this is done depends on the needs of each individual medical center but provides a strong connection between the goals of the facility and drives the control of resources down to the service level. The ease of user and single point of information aids service level management in increasing their business acumen.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

None. 4Cast does not derive or create new data records regarding the information received and there is no additional analytics performed automatically to drive decision making. Instead, 4Cast brings data from several systems into a single view and provides a bottoms-up estimate of resource needs. This single view of data allows decision makers to more easily see the total needs of the facility and allocate resources effectively.

2.3 How is the information in the system secured?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

All 4Cast users have access to the same information, but only users involved in the planning process or Fiscal staff have access to 4Cast. User accounts are unlimited, but all requests go through an on-site administrator (usually the CFO or someone else appointed on the Fiscal staff) and all requests are then routed to the 4Cast Support Staff for approval. Additionally, the only PII within 4Cast is masked or not displayed to end users.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

All 4Cast users have access to the same information, but only users involved in the planning process or Fiscal staff have access to 4Cast. User accounts are unlimited, but all requests go through an on-site administrator (usually the CFO or someone else appointed on the Fiscal staff) and all requests are then routed to the 4Cast Support Staff for approval. Additionally, the only PII within 4Cast is masked or not displayed to end users.

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

The information listed in section 1.1 is retained as follows:
Employee Name – masked
Employee ID – converted

No other information from Section 1.1 is stored/retained in 4Cast.

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?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The data in Section 1.1 is retained for a maximum of three years within 4Cast. All prior records are retained indefinitely in a protected snapshot within the AWS GovCloud RDS structure. All business plans and monitoring information are maintained within 4Cast and accessible online for a minimum of three years and a maximum of 5 years. After 3 years, the FTEE individual record data is archived and stored indefinitely in an AWS backup snapshot. Summary data is retained as necessary up to 5 years.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.
4Cast does not allow the retrieval of a record via a personal identifier and also is not the system of record for this information. Therefore, the NARA requirements do not apply.

3.4 What are the procedures for the elimination of SPI?

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

4Cast only receives, processes, and stores electronic records and therefore no records are destroyed at the end of the retention period. All historical records are retained indefinitely as a database snapshot at a minimum annually.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

No data in 4Cast is stored in any format different than listed above. If data is required for testing or training, the masking of Employee Name is increased from Smith, Joh*** to ***,***. As previously stated, because Employee Name is rolodex information, there is no additional risk to privacy related to testing or training environments.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
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 are no risks associated with the retention of the information in 4Cast since the information does not uniquely identify individuals. 4Cast protects the information collected in Section 1.1 (Employee name and Employee ID) by masking and conversion so that the initial data is no longer stored in the original format.

Mitigation: Cast retains Section 1.1 data for a maximum of three years for online processing and storage and after that time the data is archived

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
N/A			

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: N/A.

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

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

N/A.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Mitigation: N/A.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is 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.

On the login page for 4Cast, the following disclosure exists per the guidance of OI&T:

Reminder: No PHI (Protected Health Information), or PII (Personally Identifiable Information) is to be entered into the system (https://4cast.plan4hc.com).

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

The information collected by 4Cast is service level business planning information and is not privacy information, SPI or PII. The individuals are explicitly instructed not to enter PII or PHI into 4Cast.

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

The information collected by 4Cast is service level business planning information and is not privacy information, SPI or PII or related to the individual entered data. The individuals are explicitly instructed not to enter PII or PHI into 4Cast.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Follow the format below:

Privacy Risk: There are no risks associated with the information since no individual SPI or PII is collected or maintained in 4Cast and the data is not for individual use or identification.

Mitigation: The information collected by 4Cast is service level business planning information and is not privacy information, SPI or PII. The individuals are explicitly instructed not to enter PII or PHI into 4Cast.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

4Cast is contracted by VA per a license agreement which stipulates that the data within 4Cast is owned by VA. At any time, a medical center can request a full download or summary report of the data in 4Cast and the support staff will provide. Additionally, per our contractual requirements, Plan 4 Healthcare will comply with all VA FOIA regulations.

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.

4Cast provides a single point of contact for all users: 4castsupport@plan4hc.com. Any issues with reported inaccurate information – the issue will be documented in the email and the data re-processed with any relevant changes.

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.

No individual SPI or PII is collected or maintained in 4Cast and therefore this control is not applicable to individuals.

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

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

No individual SPI or PII is collected or maintained in 4Cast and therefore this control is not applicable to individuals.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?
Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: N/A.

Mitigation: N/A.

Section 8. Technical Access and Security

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

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

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

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

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

User accounts are unlimited, but all requests go through an on-site administrator (usually the CFO or someone else appointed on the Fiscal staff) and all requests are then routed to the 4Cast Support Staff for account creation. Login instructions are then sent directly from the 4Cast Support Staff to the user individually. There are three roles within 4Cast available to users: User: has access to make changes to a service(s) business plans and view monitoring data. Once business plans are submitted, the plan is read-only, and no further changes are allowed.

Admin: Admin users have access to all business plans within a facility and have read/write access. In addition, admin users have access to all internal reporting within 4Cast.
ViewOnly: ViewOnly users have access to all business plans within a facility and have read-only access.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA Contractors do not have access to 4Cast and do not have input into the design and maintenance of the system.

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.

All VA employees are required to attend annual privacy and security training. Those controls apply to 4Cast and a disclosure reminder regarding PHI and PII is displayed on the login page.

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

If Yes, provide:

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

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

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

4Cast has a current ATO with conditions signed May 14, 2021 for 90-days. FIPS 199 classification of 4Cast is Low.

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes, the system uses Amazon Web Services (AWS) as the infrastructure provider and the 4Cast solution is hosted on the Amazon US-GOV-WEST-1 cloud. In May 2021, 4Cast was determined to be a Managed Service provider for VA as it only met 3 of the 5 criteria for Software as a Service. 4Cast does not have a FedRAMP authorization as it only provides services to VA as a government agency.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Managed Service - SaaS

9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

All existing contracts for 4Cast licensing specify that VA is the sole owner of the data and that 4Cast is a steward of the data.

9.4 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.

Neither 4Cast nor the Cloud Services Provider (AWS) collects any ancillary data. Any data collected is owned by VA.

9.5 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.

Yes, all contracts for 4Cast licensing specify that 4Cast is required to abide by all applicable VA security requirements and controls. 4Cast as a Managed Service manages the security of the organizational data that is provided in accordance with these requirements.

9.6 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).

No, 4Cast does not employ the use of Robotics Process Automation (RPA) or any other type of AI or Machine Learning.

Section 9. 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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Andrea J. Wilson 104706

Digitally signed by Andrea J. Wilson 104706
Date: 2021.07.28 17:15:03 -04'00'

Privacy Officer, Wilson, Andrea

JEFFERY M. ROSS 111640

Digitally signed by JEFFERY M. ROSS 111640
Date: 2021.07.28 15:23:29 -06'00'

Information Systems Security Officer, Ross, Jeff

LARRY T. WILDES 186749

Digitally signed by LARRY T. WILDES 186749
Date: 2021.08.03 11:38:35 -06'00'

System Owner, Wildes II, Larry

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).

4Cast link: https://4cast.plan4hc.com