



Privacy Impact Assessment for the VA IT System called:

Press Ganey

VHA

VA Northeast Ohio Healthcare

Date PIA submitted for review:

October 5, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Joseph Picklo	joseph.picklo@va.gov	(216) 791-2300 x 42341
Information System Security Officer (ISSO)	Amine Messaoudi	amine.messaoudi@va.gov	(202) 815-9345
Information System Owner	Ruth Hatchuel	ruth.hatchuel@va.gov	216-791-2300 x 42126
Record Officer	Carnelle Stafford Sr.	Carnelle.stafford@va.gov	216-7912300 X 45304

Abstract

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

Press Ganey (PGA) is a third-party contractor that conducts patient experience surveys. They include several surveys as listed below which incorporate the “Consumer Assessment of Healthcare Providers and Systems” (CAHPS) questions as well as standardized Press Ganey and VA customized questions. These surveys are either mailed out (hard copy) or sent via e-mail (digitally). In Patient surveys are sent out 45 days after the Survey of Healthcare of Patients (SHEP) survey has have been mailed. The Outpatient, Emergency Department, Outpatient Mental Health, Supportive Services and Ambulatory Surgery surveys are sent electronically within 24-48 hours after their appointment/visit. (Patients will only receive one survey per 3-month period). CLC (Nursing home) survey is provided to residents every other month and is administered by the Patient Liaisons to Veterans who need assistance. A section of the Senior Executive Service Plan (SES) requires the provision, analysis of and responses related to Patient Experience Satisfaction data. This product provides a comprehensive survey, measurement, deep dive analysis, and reporting of patient experience and patient satisfaction for the VA Northeast Ohio Healthcare System (VANEOHS) as a whole the results allow for, customized and standard reports of patient experiences and provide opportunities and information for improvement plans to be developed, implemented and evaluated.

Overview

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

1 General Description

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

“Press Ganey” IT system owned by Press Ganey Inc. but operated through the VANEOHS – Employee/Patient Experience Service.

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

With the new Mission Act and Veteran access to Community Care it is essential that we ascertain how each service or unit/ service /provider is functioning and meeting or exceeding benchmarks hence we require that patient satisfaction data be reported at the unit /service / individual (provider) level and benchmarked to a national source.

The survey tool and associated reporting database, enables collection and analysis of provider-specific patient satisfaction data and benchmarking of data to a comprehensive database of leading health care institutions patient satisfaction performance utilizing the same tools at each facility. An evidence-based survey tool allows for inclusion of customized questions and Veteran comments. The system enables the measurement of patient satisfaction for all providers and services at the VANE OHS. PGA customizes facility-wide measurement of patient satisfaction survey instruments for specified units/clinics/ providers and supportive services at the VANE OHS, which SHEP does not.

The primary objective of this survey tool is to identify the root causes or areas of weakness enabling us to improve our services, ultimately increasing satisfaction of patients during their hospitalization or while receiving outpatient or long-term care from the VANE OHS, thus keeping our Veterans selecting VA as their healthcare provider of choice. The results are used to gain insight on the opinions of Veterans who use services in VANE OHS. The tool provides front line staff with real time feedback on patient perceptions and offers solutions to improve employee performance and enhance our delivery of outstanding and quality care.

The secondary objective is to benchmark VANE OHS aggregated and unit-level performance against other healthcare systems, to include both VA and Non-VA systems across the country which is needed for Pathways and magnet designation. (SHEP and Vsignals only compares VA to VA).

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

Ownership of this tool is with Press Ganey, however VANE OHS provides the data required to send out the surveys and create the reports.

2. Information Collection and Sharing

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

The typical client or affected individual is a Veteran patient that would have an encounter for a test/treatment/medical appointment/inpatient stay /emergency room visit AND was selected to receive a survey. Approximately 273,000 patient records were sent surveys in a 12-month period. Note: these may not be unique patient records as patients may receive multiple survey types or multiple attempts for sending surveys. Patient records are stored for 10 years.

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

This is a survey that processes information based on a veteran's responses to the questions asked. These questions have a likert scale and "yes and no" responses as well as comment sections for Veterans to record their responses. The primary objective of this survey tool is to identify the root causes or areas of weakness enabling us to improve our services, ultimately increasing satisfaction of patients during their hospitalization or while receiving outpatient or long-term care from the VANE OHS, thus keeping our Veterans selecting VA as their healthcare provider of choice. The results are used to gain insight on the opinions of Veterans who use services in VANE OHS. The tool provides front line staff with real time feedback on patient perceptions and

offers solutions to improve employee performance and enhance our delivery of outstanding and quality care.

The secondary objective is to benchmark VANE OHS aggregated and unit-level performance against other healthcare systems, to include both VA and Non-VA systems across the country. (SHEP only compares VA to VA).

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

Patient demographic data is sent to Press Ganey via SFTP to the Data Ingress application. Press Ganey processes that incoming data and generate paper, phone, and web-based surveys. Patients provide survey responses which may include unstructured comments. Results of those surveys are summarized and provided back to the VA via PGFusion and Narrative Dx.

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

The system is hosted in AZURE Commercial Cloud and is currently used by VANE OHS.

3. Legal Authority and SORN

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

5 USC 552a, The Privacy Act of 1974, 38 USC 5701 Confidentiality Nature of Claims, SORN 121VA10, National Patient Database

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

The system uses cloud technology and is covered by the SORN.

https://www.oprm.va.gov/privacy/systems_of_records.aspx

National Patient Databases-VA (121VA10)

D. System Changes

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

It will not require changes to business processes

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

It will not result in technology changes

Section 1. Characterization of the Information

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

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

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

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

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

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

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

(Press ganey to help answer this question)

Name

Social Security

Number

Date of Birth

Mother's Maiden Name

Personal Mailing

Address

Personal Phone

Number(s)

Personal Fax Number

Personal Email Address

Emergency Contact

Information (Name, Phone Number, etc. of a different individual)

Financial Information

Health Insurance

Beneficiary Numbers

Account numbers

Certificate/License numbers*

Vehicle License Plate Number

Internet Protocol (IP)

Address Numbers

Medications

Medical Records

Race/Ethnicity

Tax Identification Number

Medical Record Number

Gender

Integrated Control Number (ICN)

Military History/Service

Connection

Next of Kin

Other Data Elements

Internal Entry Number (IEN)

PII Mapping of Components (Servers/Database)

Press Ganey consists of “1” key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Press Ganey and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CPRS / Vista	yes	no	Veteran’s Name, Patient IEN, address, e-mail address, phone number, Clinical Trainees and employee Name	To send out surveys to Patients’ who have visited the VA in the In-Patient and outpatient settings as well as long Term Care.	All PII within the Press Ganey application is protected by Administrative, Technical, and Physical controls under FedRAMP security baselines such as Principle of least privilege, security controls, etc.

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

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

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

We use Vista to identify patients and process to send out surveys to patients who have visited the VA as an In-patient, for Outpatient or Long-Term Care.

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.

Vista provides patient information so that it can be sent to a third-party surveyor (Press Ganey) randomly to avoid asking the patient for the information / responses.

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

No other systems create additional information for Press Ganey

1.3 How is the information collected?

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

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

There is a Security File transfer protocol (SFTP) transmission from VISTA to Press Ganey.

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

Information is not collected on a form

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

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

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

Press Ganey provides multiple quality controls checks for ensuring accuracy in the various micro-flows of the data collection process including but not limited to: Quality checks on the test files from the VA and duplicate checks for records of patients already sample; manually clarification of questionable or conflicting information during data collection/receipt.

Press Ganey uses the Pitney Bowes Finalist® software, a Coding Accuracy Support System (CASS) Certified application, to check for valid addresses. Finalist software corrects and standardizes street names, suffixes, city names, states, zip codes and ZIP + 4® codes. It then adds carrier and delivery point information.

Press Ganey also implemented the use of the Pitney Bowes Verimove® software which accesses the United States Postal Service (USPS) National Change of Address (NCOA) database. All CASS Certified addresses are checked against the NCOA database and updated addresses are used for mailing.

Press Ganey stores the address from the NCOA database, the CASS Certified address, and the address supplied by the client.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

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

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

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

This is an IT system which collects, processes, retains, or shares PII/PHI information and requires a new PIA within 60 days from last dated signature. The Press Ganey is a privacy sensitive system that collects, maintains, and/or processes Personally Identifiable Information on Veterans and/or dependents, VA employees and clinical trainees. A Business Associate Agreement and Memorandum of Understanding is in place. Legal authority also consists of 5 USC 552a, The Privacy Act of 1974, 38 USC 5701 Confidentiality Nature of Claims, SORN 121VA10, National Patient Database

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section) Amine Messaoudi to complete.

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:

Press Ganey contains sensitive personal information – including names and addresses on veterans. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm, or even identity theft may result.

Mitigation:

Veterans’ Health Administration (VHA) deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within VHA to include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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.

Veterans name – used to access the information from VISTA for survey mailing purposes.

Version Date: October 1, 2022

Page 9 of 33

Veterans Gender, Race and Ethnicity and Date of Birth – for analytics purposes
Veterans Address– used to access the information from VISTA for survey mailing purposes.
Veterans E-Mail address– used to access the information from VISTA for survey mailing purposes.

Veterans Phone number– used when the Veteran provides his /her name and phone number on the returned survey so employee can call Veteran to obtain further information related to their comments.

Employee Name and e-mail address – Used to connect Veteran to their care giver and location of visit, and for Report creation.

Clinical Trainee name and e-mail address - Used to connect Veteran to their care giver and location of visit.

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

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Elements include performing analysis using Press Ganey and manual exports this includes mean ratings, sample sizes, response rates, trending, statistically significant results, external (non-VHA) comparisons, correlation analysis, other demographic variables, as well as priority index and non-structured comments. Benchmarking to the commercial sector is available with access to a variety of peer groups as well as VA specific peer groups.

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.

Press Ganey does not create new demographic information about individuals. Survey responses are associated with individuals and summarized in aggregations. VA has access to the summary data and can see individual survey response data.

2.3 How is the information in the system secured?

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

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

Personal information is transmitted from VA to Press Ganey via SFTP. A national MOU ISA is in place covering this interconnection. Once received by Press Ganey, all VA data is encrypted at rest and in transit over public networks. Press Ganey has implemented a mature security program covering all key domains of a security program, including access management, endpoint security, logging and monitoring, and incident response.

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

The system is not collecting SSN's

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

Personal information is transmitted from VA to Press Ganey via SFTP. A national MOU ISA is in place covering this interconnection. Once received by Press Ganey, all VA data is encrypted at rest and in transit over public networks. Press Ganey has implemented a mature security program covering all key domains of a security program, including access management, endpoint security, logging and monitoring, and incident response.

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?

Employee name is entered into the Press Ganey management system by the system Administrator. The System administrator designates the access according to the employee role and location of work.

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

The System administrator designates the access according to the employee role and location of work.

2.4c Does access require manager approval?

Access requires both manager and System Administrator approval

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

Yes, access is monitored by the System Administrator. When an employee leaves the institution or changes roles within the system they will be removed from the system or reassigned according to their new role

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

VA System Administrator and Press Ganey Security

Section 3. Retention of Information (Press Ganey to complete)

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- Name
- Date of Birth
- Personal Mailing Address
- Personal Email Address
- Race/Ethnicity
- Gender
- Unstructured verbatim comments

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

Press Ganey retains personal information about VA patients for 10 years after the survey is sent, or until the end of our relationship with the VA, whichever is sooner. Each discharge/survey is treated individually, so if Press Ganey receives the same personal information several times, only the data received more than 10 years ago is deleted.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

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

The Records Control Schedule (RCS) 10-1 provides Veterans Health Administration (VHA) records retention and disposition requirements for VHA Central Office, Program Offices, and field facilities. The primary purpose of this revision is to incorporate changes to RCS 10-1 issued since the last publication date of January 2019. The schedule is divided into eight chapters. Each chapter covers a group of records, e.g., chapter one covers administrative records. The first four chapters include most of the National Archives and Records Administration (NARA) General Records Schedules (GRS). Space for additional records schedules is available to allow for future expansion. The VHA Records Management Office intends to update this schedule every three years in order to publish the most up to date records management requirements. Between updates the VHA Records Management Office will post new or revised schedules on the HIM/RM (Health Information Management/Records Management) website. Schedules are not required to be in the RCS 10-1 to be a legal schedule. Once a schedule is approved by the Archivist of the United States it must be used to manage the agency's records.

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

The VHA Records Control Schedule (RCS) 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service [rcs10-1.pdf \(va.gov\)](#).

General Administration & Management Records; Series 1001 thru 1950

Information Technology; Series 2000 thru 2525

Civilian Personnel; Series 3010 thru 3400

Employee Training Records; Series 3400

Financial Management; Series 4000 thru 4110

Logistics and Facilities; Series 5020 thru 5700

Healthcare Records; Series 6000 thru 6675

Ancillary Services; Series 7000 thru 7950

Office of Research and Development; Series 8000 thru 8600

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.

After 10 years, personal information and survey response data is deleted from Press Ganey systems using logical deletion techniques. When media reaches end of life, Press Ganey destroys or sanitizes physical media using the guidelines in the NIST Special Publication 800-88, Guidelines for Media Sanitization or its successor. In accordance with VA Directive 6500, Cyber Security Program, VA Handbook 6500, VA Information Security Program, VA Directive 6300, Records and Information Management

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.

Employees who use the system are trained on how to create reports and manage the results through a formal training program provided by the System Owner and trained trainers.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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 is a risk that the information maintained by Press Ganey will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: Press Ganey's mature security program protects all personal information. Per the Business Associate Agreement, paragraph M, the contractor: Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy, as determined by and under the direction of Covered Entity all PHI created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If

return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the Agreement and use or disclose the information only for the purpose of making the return or destruction feasible, or as required by law or specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

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

<i>List the Program Office or IT System 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 the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Veterans Health Administration, VISTA	For evaluating perception of veteran’s care	Patient name, Address, e-mail address, DOB, Race/ethnicity and gender	Electronically pulled from VISTA thru Computerized Patient Record System (CPRS)
Veterans Administration, Microsoft Outlook	To process surveys	Name and e-mail address	TIC

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for evaluating perception of Veterans care. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: Shared data within the organization is controlled through system access management.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

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

Data Shared with External Organizations

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
Data Ingress	To formulate patient surveys	Name, address, e-mail address, phone number	MOU ISA. BAA	SFTP

PG Fusion	To formulate and process patient surveys	Name, address, e-mail address, phone number	BAA	Vendor internal processing
National Database of Nursing Quality Indicators (NDNQI)	To request survey data	No PHI /PII. Only de-identified information and aggregate information	Data Use Agreement	SFTP
Survey Solutions and Survey Processing	To process and facilitate patient surveys	Name, address, e-mail address, phone number	BAA	Vendor internal processing
eSurvey and SMS Text Invitations	To request survey data from patients	Name, address, e-mail address, phone number	BAA	Vendor internal processing

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.

Press Ganey VA National MOU ISA 2021.08.23 – Fully Signed and Executed w Annual Review, last reviewed 2023.06.21 (see attached)

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: Due to the sensitive nature of this data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal,

and/or financial harm may result for the affected individuals. VA would be required to provide credit monitoring and ID theft insurance.

Mitigation:

Personal information is transmitted from VA to Press Ganey via SFTP. A national MOU ISA is in place covering this interconnection. Once received by Press Ganey, all VA data is encrypted at rest and in transit over public networks. Press Ganey has implemented a mature security program covering all key domains of a security program, including access management, endpoint security, logging and monitoring, and incident response.

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Veteran receives a cover letter together with each survey that is sent out either by post or e-mail. This cover letter explains what the survey is for and provides a privacy notice as well. The Notice states: “Your information will be protected under 5 USC 552a, The Privacy Act of 1974, 38 USC 5701, and the HIPAA Privacy Rule. Press Ganley has entered into a Business Associate Agreement which legally compels them to protect your information”.

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

Notice was provided – sample attached in Appendix A 6.1

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

See attached cover letter in Appendix A 6.1 – this is to inform the Veteran that their responses will remain confidential and will only be used for the sole purpose of evaluating our service to them. We do not share their information with others outside of the contracted third-party survey company (Press Ganey) and the VA.

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.

Yes, the individual does have the right to decline / not complete and return the survey. There are NO penalties or denials of service for not completing the survey.

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 individual does not need to answer all survey questions and has the right to provide comments. They also are not required to share their name or phone number as part of the survey returned. This is purely optional.

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

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

Principle of 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: The risk for not providing notice would be a lack of transparency for the patient not being aware of the system's use of information.

Mitigation: A privacy notice must be acknowledged each patient initiates a survey.

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

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

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at <http://www.foia.va.gov/> to obtain information about FOIA points of contact and information about agency FOIA processes.

If the patient wanted personal / personal record information they would complete a Privacy Act or Freedom of Information Act request. They would start at the Patient advocate office to assist with the process.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

The system is not exempt from the Privacy Act access provision.

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.

If the patient wants personal record information, they would be required a Privacy Act or Freedom of Information Act request. They would start at the Patient Advocate office to assist with the process.

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.

If the patient wants personal record information they would complete the FOIA process. They would start at the Patient advocate office to assist with the process.

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.

The Veteran would be instructed on the procedure through the Advocate Office

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

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.***

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

Not applicable

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

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

Privacy Risk: There is a risk that individuals are unaware of how to access or correct their information in the system.

Mitigation: The Veteran would receive this information through the Advocate office. The Advocate would contact / consult the Privacy Officer to begin the mitigation process.

Section 8. Technical Access and Security

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

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

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

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

Employee is enrolled onto the Press Ganey management system by the system Administrator. The System administrator will then designate access according to the employee role and location of work.

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?
No other agencies have access to the system

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

A standard user has access to view data, create reports using specific data as needed.

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.

Press Ganey is the contractor and has a BAA and MOU ISA in place with the VA regarding roles and responsibilities

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 users of the system are VA employees, therefore, yearly training is required for all users including additional training for managing PII and paperwork for PII including VA Privacy and information security awareness and rules of behavior and Annual Government Ethics Training. Press Ganey is the contractor and has a BAA and MOU ISA in place with the VA regarding their roles and responsibilities

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 7/11/2023*
3. *The Authorization Status: Authorized to Operate*
4. *The Authorization Date: 9/5/2023*
5. *The Authorization Termination Date: 3/03/2024*
6. *The Risk Review Completion Date: 8/10/2023*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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

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

N/A

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.

Version Date: October 1, 2022

Page 25 of 33

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

Press Ganey's software is hosted in both a co-located data center where hardware is managed by Press Ganey, and within Microsoft Azure, where hardware is managed by Microsoft. Both Press Ganey and Microsoft have mature security programs designed to protect personal information. Neither Press Ganey nor Microsoft have received FedRAMP authorization for the in-scope services.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). *(Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers*

Press Ganey is the contractor and has a BAA and MOU ISA in place with the VA regarding their roles and responsibilities

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.

Press Ganey collects survey responses including unstructured comment data. This data belongs to the VA.

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.

This information is included in the MOU ISA

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).

Press Ganey does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Version Date: October 1, 2022

Page 28 of 33

ID	Privacy Controls
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, Joseph Picklo



Information System Security Officer, Amine Messaoudi

Information System Owner, Ruth Hatchuel

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).

6.1a Cover letter for Press Ganey On-line Survey

  **U.S. Department of Veterans Affairs**
Veterans Health Administration
VA Northeast Ohio Healthcare System

Dear {FIRST_NAME} {LAST_NAME},

VA Northeast Ohio Healthcare System is constantly working to enhance and improve our healthcare environment. To ensure we are focused on the right priorities, VA has contracted with Press Ganey, a recognized leader in healthcare performance improvement with more than 25 years of experience. Press Ganey has worked with more than 10,000 healthcare organizations nationwide, including 50 percent of all U.S. hospitals to improve their clinical and business practices.


The following is a 5 to 10-minute questionnaire about your most recent healthcare visit. We hope you will take the time to fill it out to help us improve upon the service we deliver you and your fellow Veterans. Your response will be confidential, so please answer the questions as honestly as possible.

Thank you for taking the time to provide us with your valuable feedback.

Your information will be protected under 5 USC 552a, The Privacy Act of 1974, 38 USC 5701, and the HIPAA Privacy Rule. Press Ganey has entered into a Business Associate Agreement which legally compels them to protect your information.

Should you have any questions about the survey, feel free to contact the Patient Advocate Office at 216-791-3800 ext. 61700, Monday – Friday from 8 a.m. to 4 p.m.

Sincerely,


Jill Dietrich Mellon, JD, MBA, FACHE
Executive Director / CEO

[Start Survey](#)



VA NORTHEAST OHIO HEALTHCARE SYSTEM
U.S. DEPARTMENT OF VETERANS AFFAIRS
19701 EAST BOTTLERYARD
CLEVELAND, OH 44106

SURVEY INSTRUCTIONS: You should only fill out this survey if you were the patient during the hospital stay named in the cover letter. Do not fill out this survey if you were not the patient. Answer all the questions by completely filling in the circle to the left of your answer. You are sometimes told to skip over some questions in this survey. When this happens you will see an arrow with a note that tells you what question to answer next, like this:

Yes

No → **If No, Go to Question 1**

Please answer the questions in this survey about your stay at VA Northeast Ohio Healthcare System. Do not include any other hospital stays in your answers.

YOUR CARE FROM NURSES

1. During this hospital stay, how often did nurses treat you with courtesy and respect?

- Never
 Sometimes
 Usually
 Always

2. During this hospital stay, how often did nurses listen carefully to you?

- Never
 Sometimes
 Usually
 Always

3. During this hospital stay, how often did nurses explain things in a way you could understand?

- Never
 Sometimes
 Usually
 Always

4. During this hospital stay, after you pressed the call button, how often did you get help as soon as you wanted it?

- Never
 Sometimes
 Usually
 Always
 I never pressed the call button

YOUR CARE FROM DOCTORS

5. During this hospital stay, how often did doctors treat you with courtesy and respect?

- Never
 Sometimes
 Usually
 Always

6. During this hospital stay, how often did doctors listen carefully to you?

- Never
 Sometimes
 Usually
 Always

7. During this hospital stay, how often did doctors explain things in a way you could understand?

- Never
 Sometimes
 Usually
 Always

THE HOSPITAL ENVIRONMENT

8. During this hospital stay, how often were your room and bathroom kept clean?

- Never
 Sometimes
 Usually
 Always

9. During this hospital stay, how often was the area around your room quiet at night?

- Never
 Sometimes
 Usually
 Always

YOUR EXPERIENCES IN THIS HOSPITAL

10. During this hospital stay, did you need help from nurses or other hospital staff in getting to the bathroom or in using a bedpan?

- Yes
 No → **If No, Go to Question 12**

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)