The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Huron Accelerators Platform

Tennessee Valley Medical Center
Veterans Health Administration

Date PIA submitted for review:

08/24/2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Robbie Braswell</td>
<td><a href="mailto:Robbie.braswell@va.gov">Robbie.braswell@va.gov</a></td>
<td>615-225-5417</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Andrew Vilailack</td>
<td><a href="mailto:Andrew.vilailack@va.gov">Andrew.vilailack@va.gov</a></td>
<td>813-970-7568</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Fred Tolley</td>
<td><a href="mailto:Fred.tolley@va.gov">Fred.tolley@va.gov</a></td>
<td>202-461-9005</td>
</tr>
</tbody>
</table>
Abstract

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

The Huron Accelerators Portal (HAP) is a web-based entry portal, hosted on AWS GovCloud. HAP is composed of three components: the Leader Evaluation Manager® (LEM) software application, the Patient Call Manager™ (PCM) software application, and the Huron Rounding software application. Respectively, the three components function as tools for leadership evaluation, the facilitation of patient discharge follow-up, and the collection of improvement opportunities.

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?

Huron Accelerators Platform (HAP) is a web-based entry portal into the Huron Healthcare Accelerator system. Depending on which modules a customer has purchased, HAP allows access into the customer’s systems with the appropriate options and permissions. The modules are detailed below. The business owner and creator of the tool is Huron Consulting Services LLC (“Huron
Consulting Services”). Pursuant to Contract Number 36C24918CO193, Huron Consulting Services and its subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks.

Pursuant to Contract Number 36C24918C0193, Huron Consulting Services LLC and its subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks.

The completion of this PIA will not result in circumstances that require changes to VA technical or business processes. The Huron Rounding application resides in the AWS Gov Cloud environment. The AWS GovCloud has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for high impact level. The VA owns all data stored in the PCM software per Contract Number 36C24918C019 and 36C24618Q09860. Refer to AWS privacy resources for more information on Compliance, Privacy and Security for the Gov Cloud. (see https://aws.amazon.com/compliance/data-privacy-faq/)

The magnitude of potential harm if privacy related data is disclosed is high, due to the potential for identity theft. The reputation of both Huron Consulting Services LLC and VA could be negatively impacted by a privacy related data disclosure as Veteran information is stored in the databases, as defined in this PIA. The number of patient records stored can vary, depending on discharge volume.

LEADER EVALUATION MANAGER

The Leader Evaluation Manager® (LEM) application is a Software as a Service (SaaS) tool that will be used by Tennessee Valley Healthcare System. The LEM tool is designed to drive accountability within VA leadership by allowing leaders to enter, access, and share goals and progress data transparently and efficiently.

Authorized Users access the Leader Evaluation Manager application through a secure web portal authentication and can view the following data elements:

- First Name, Last Name, Email Address, Department, Division, Job Title, Direct Supervisor, Hire Date, goals, action plans

It is expected that approximately 160 Tennessee Valley Healthcare System leaders will utilize the LEM application and non-sensitive information related to goals, action plans, and goal progress could be shared internally and externally with authorized Huron coaches.

LEM does not share information with any other IT System. As a vendor hosted multi-tenant Software as a Service tool, data segregation between locations is enforced logically within the system at the application and database layer. The Leader Evaluation Manager application is hosted on the AWS GovCloud usgov-west-1 region with the east Region as the designated disaster recovery region as of July 24, 2019.
The completion of this PIA will result in new business processes and technology changes by organization leaders to utilize LEM to align their goals and action plans for operational improvement. The LEM tool meets requirements in order to comply with VA Handbook 6517 and is currently in-process to receive FEDRAMP certification and ATO.

PATIENT CALL MANAGER

The PCM application is a Software as a Service tool designed to streamline the tactic of ‘transition of care’ phone calls. Implementing transition of care phone calls is a statistically proven technique to improve clinical outcomes and patients’ perception of care. The PCM tool will be used by Tennessee Valley VA Healthcare System clinical staff.

Authorized Users access the Patient Call Manager application through a secure web portal authentication and can view the following data elements:

- Employee Data: First Name, Last Name, Email Address, Department, Division, Job Title
- Patient Data: Medical Record Number, Preferred Language, Sex, Visit Number, Status, Admit Date, Service Date, Admitting Diagnosis, Nursing Unit Name, Procedure Name, Attending Physician Name, patient survey responses.

It is expected that approximately 50 Tennessee Valley VA clinical staff will utilize PCM. The number of individuals with information stored in the system is dependent upon patient discharge volume.

HURON ROUNDING

The Huron Rounding tool is a web-based commercial SaaS application designed for healthcare professionals, which allows them to standardize, automate, and track rounding activities. Nursing and or other clinical staff may use the application to gather subjective data from patients on their hospital experience via an electronic survey. This survey will provide information the hospital leaders can use to assess patient satisfaction.

The categories of individuals with records in this system are VA health care beneficiaries and other categories of individuals who receive medical treatment at VA treatment facilities/activities. Survey data is collected in the patient’s room via a mobile device or computer, and data remains within the collection instrument. The unidentified data is aggregated in reports. Patient Rounding is administered to a random population of the total number of patients, the volume of which cannot be stated with certainty.

Medical center leader information is also included in the system. A total of 160 leaders from Tennessee Valley Healthcare System are expected to have data stored in the system. This number is subject to change as hiring changes.
Huron was informed by the VA PIA team that the following SORNs are applicable to Leader Evaluation Manager® (LEM), Patient Call Manager™ (PCM), and Huron Rounding:

Patient Medical Records–VA (24VA10P2)
Veterans’ Health Information Systems and Technology Architecture (VistA) Records–VA (79VA10)

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://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)
Veterans or Dependents
MyRounding®: Department, Facility, Room, Bed, First name, Last name, Discharge Date, Date of Birth, Medical Record Number, Patient Code, Patient Visit ID, Prior Patient Code, Prior Visit ID, patient rounding responses.

PCM: Name, Date of Birth, Phone Number, Race, Medical Record Number, Preferred Language, Sex, Visit Number, Status, Admit Date, Service Date, Admitting Diagnosis, Nursing Unit Name, Procedure Name, Attending Physician Name, Patient Survey Responses

VA Employees
MyRounding® Staff Rounding: Employee Name, Email address, Location/Department, Direct Reporting employees, Rounding responses

PCM: Name, Email Address, Department, Division, Job Title

LEM: Name, Email, Address, Department, Division, Job Title, Direct Supervisor, Hire Date, Goals, Action Plans

VA Contractors
MyRounding® Staff Rounding: Employee Name, Email address, Location/Department, Direct Reporting employees, Rounding responses

PCM: Name, Email Address, Department, Division, Job Title

LEM: Name, Email, Address, Department, Division, Job Title, Direct Supervisor, Hire Date, Goals, Action Plans

Members of the Public/Individuals
MyRounding®: Department, Facility, Room, Bed, First name, Last name, Discharge Date, Date of Birth, Medical Record Number, Patient Code, Patient Visit ID, Prior Patient Code, Prior Visit ID, patient rounding responses

PCM: Name, Date of Birth, Phone Number, Race, Medical Record Number, Preferred Language, Sex, Visit Number, Status, Admit Date, Service Date, Admitting Diagnosis, Nursing Unit Name, Procedure Name, Attending Physician Name, Patient Survey Responses

Clinical Trainees
MyRounding® Staff Rounding: Employee Name, Email address, Location/Department, Direct Reporting employees, Rounding responses

PCM: Name, Email Address, Department, Division, Job Title

LEM: Name, Email, Address, Department, Division, Job Title, Direct Supervisor, Hire Date, Goals, Action Plans
PII Mapping of Components

Huron Accelerators Platform consists of 3 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Huron Accelerators Platform 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.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS GovCloud</td>
<td>Yes</td>
<td>Yes</td>
<td>Employee Data</td>
<td>Goal Entry -- Utilized to establish, monitor and evaluate performance against identified goals of the leader. Administration -- Required for setting role-based permissions and associating employees to action plans. Reports -- Used so that the application can return report results specific to the individual.</td>
<td>AWS GovCloud</td>
</tr>
</tbody>
</table>
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.

LEADER EVALUATION MANAGER

Leaders within the VA organization provide the specific information above. All data elements are collected from the employee and their supervisor; there is no information collected from other sources. Organizational goals are created by senior leaders and cascaded to all leaders to ensure accountability. Information is collected by individual leaders as they comment on their progress towards goals throughout the year.

Some data elements are created by the Leader Evaluation Manager tool in the form of reporting including aggregation of goals into a single Excel-exportable report.

PATIENT CALL MANAGER

Many data elements are collected via File Transfer Protocol Secure (FTPS) /SSH File Transfer Protocol (SFTP) data extract from each medical center’s VistA system, including patient first name, last name, phone number, visit number, admit date, service date, admitting diagnosis, nursing unit name, and attending physician name. These data elements serve as the basis of the work driver for callers to have the critical data to ask informed questions of patients. This information must be obtained prior to patient contact so that the patient can be reached over the phone.

Some data elements are collected directly from the individual. Patient responses to post-visit call surveys could include health information, care instructions, and other diagnosis/procedure related information. Survey responses are documented by the nurse or caller into the system, and the Veteran/individual does not enter responses to a web form directly.

Some data elements are created by the Patient Call Manager application in the form of call statistics reporting.
HURON ROUNDELING

Huron Rounding will be populated with data via manual entry by VA Rounding end users who are VA staff members.

Some information is collected directly from the patient during rounding conversations and then manually entered into the Huron Rounding application by the VA Rounding end users who are documenting the patient’s responses to rounding questions. Responses could include health information, care information, and other diagnosis/procedure related information. Rounding responses are documented by the person conducting the round into the system, so existing policies and procedures regarding PHI will be followed. The Veteran/individual does not enter responses directly into Huron Rounding. Information collected from the Veteran includes: Department, Facility, Room, Bed, First name, Last name, Discharge Date, Date of Birth, Medical Record Number, Patient Code, Patient Visit ID, Prior Patient Code, Prior Visit ID, patient rounding responses. Information collected during leader rounding includes leader name and rounding responses.

Some data elements are created by the clinician or leader who is conducting the round.

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.

LEADER EVALUATION MANAGER

Data elements are collected within the software user interface from the individual user.

PATIENT CALL MANAGER

Many data elements are collected via electronic transmission from VistA. Some information may be collected from the Veteran during the post-visit call and then entered into the Patient Call Manager application by the VA end user who made the post-visit call. Patient responses to post-visit call surveys could include health information, care instructions, and other diagnosis/procedure related information. Survey responses are documented by the nurse or caller into the system; the Veteran/individual does not enter responses to a web form directly.
Hurón Rounding

Data elements collected directly from patients or staff are collected during a rounding conversation and entered by a staff member into the Huron Rounding software portal.

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.

Leader Evaluation Manager

Information is collected in the LEM tool for the purpose of leader and organizational alignment. Alignment of goals supports the contract objective of “transform[ing] TVHS into a high reliability organization that consistently provides safe, efficient, effective veteran-centered care and whose employees are high-performing team players who enjoy working in the organization.”

Only information related to each leader’s goals and actions, whether publicly available or commercial, is used within the LEM. Information related to leader’s performance against goals and action plans is relevant and necessary for accountability and the execution of transforming TVHS into a high reliability organization. Goals and action plans allow for the sharing of best practices throughout the organization to other leaders with similar performance measures, and allows leaders to identify opportunities for recognition and skill development for leaders at a glance. Reporting creates the ability to drive accountability and demonstrate a common purpose through the leadership team, which will accelerate the achievement of results.

Patient Call Manager

The Patient Call Manager tool is a web-based software application designed to streamline the post-visit call process by providing hospitals with the ability to quickly and easily identify patients to call after discharge and capture call notes. Collecting individually identifiable information allows callers to directly communicate with recently discharged patients. Depending on the standardized call questions used, outcomes can include reduced readmissions and improved patient experience scores, which support the contract objective of “transform[ing]
TVHS into a high reliability organization that consistently provides safe, efficient, effective veteran-centered care and whose employees are high-performing team players who enjoy working in the organization.”

The following data elements are collected because they serve as the basis of the work driver for callers to have the critical data to ask informed questions of patients: patient first name, last name, phone number, visit number, admit date, service date, admitting diagnosis, nursing unit name, and attending physician name. Further, patient health information, care instructions, and other diagnosis/procedure related information is then collected directly from patients in order to allow the VA to manage the patient’s post-discharge healthcare in order to reduce readmissions and learn opportunities for the TVHS to improve the patient experience.

HURON ROUNDING

The Huron Rounding tool allows VA clinicians to standardize, automate, and track rounding activities. Nursing and or other clinical staff use it to gather subjective data from patients on their hospital experience via an electronic survey. This survey will provide information the hospital leaders can use to assess patient satisfaction. Improved patient experience supports the contract objective of “transform[ing] TVHS into a high reliability organization that consistently provides safe, efficient, effective veteran-centered care and whose employees are high-performing team players who enjoy working in the organization.”

With respect to patient data collected and stored in the tool, the following information may be collected from the Veteran in order to improve the patient’s experience and to allow TVHS to follow up, as needed, on the patient’s direct feedback during rounding conversations:
Department, Facility, Room, Bed, First name, Last name, Discharge Date, Date of Birth, Medical Record Number, Patient Code, Patient Visit ID, Prior Patient Code, Prior Visit ID, patient rounding responses. With respect to staff rounding, the leader’s name and rounding responses need to be collected in order to allow the VA to use such data to improve staff engagement.

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

LEADER EVALUATION MANAGER

The following legal authority applies to Leader Evaluation Manager:
Title 5: OPM/GOVT-1 through 10
(https://dvagov.sharepoint.com/sites/vacovetsprivacy/PrivacyDocuments/OPM_GOVT.pdf)
authorizes the collection of employee information by contractors performing a contracted service on behalf of VA.

PATIENT CALL MANAGER

The following legal authority applies to Patient Call Manager:

- Title 38 United States Code of Federal Regulations
  - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=828f3b1a915556ac5fd997e53930a153&tpl=/ecfrbrowse/Title38/38cfr1_main_02.tpl
  - As a Business Associate of TVHS, Huron is authorized per the Code of Federal Regulations (CFR), Title 45, § 164.504(e), to collect/use information on behalf of VA.
- Title 5, United States Code, Section 552a, "Privacy Act," c. 1974

The following SORNs are also applicable:

- Patient Medical Records–VA (24VA10P2)
- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10)

HURON ROUNDING

The following legal authority applies to Huron Rounding:

- Title 38 United States Code of Federal Regulations
  - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=828f3b1a915556ac5fd997e53930a153&tpl=/ecfrbrowse/Title38/38cfr1_main_02.tpl
  - As a Business Associate of TVHS, Huron is authorized per the Code of Federal Regulations (CFR), Title 45, § 164.504(e), to collect/use information on behalf of VA.
- Title 5, United States Code, Section 552a, "Privacy Act," c. 1974
The following SORNs are also applicable:

- Patient Medical Records–VA (24VA10P2)
- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10)

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.

LEADER EVALUATION MANAGER

**Privacy Risk:**
There is a risk that the Leader Evaluation Manager application may be compromised, resulting in a data breach involving Personal Information.

**Mitigation:**
The Leader Evaluation Manager application and architecture is designed based on modern practices technology approach which includes a least access privilege model, encryption-authentication, and account control/expiration/password change. It also utilizes key encryption security approaches per the required standard. With technology vulnerability and the risk of data being compromised rising, Leader Evaluation Manager employs full transaction logging in every aspect from end user consumption/use to all backend access by Huron staff. Logging is maintained indefinitely, setup to alert and notify on out of bound conditions and reviewed on a reoccurring basis. Furthermore, Leader Evaluation Manager has annual internal and external audits and conducts vulnerability scanning and penetration testing regularly.
PATIENT CALL MANAGER

**Privacy Risk:**
There is a risk that information could be shared with improper individuals.

**Mitigation:**
The Patient Call Manager application and architecture is designed based on modern practices technology approach which includes a least access privilege model, encryption-authentication, and account control/expiration/password change. It also utilizes key encryption security approaches per the required standard. With technology vulnerability and the risk of data being compromised rising, Patient Call Manager employs full transaction logging in every aspect from end user consumption/use to all backend access by Huron staff. Logging is maintained indefinitely, setup to alert and notify on out of bound conditions and reviewed on a reoccurring basis. Furthermore, Patient Call Manager has annual internal and external audits and conducts vulnerability scanning and penetration testing regularly.

HURON ROUNDING

**Privacy Risk:**
There is a risk that information may be accessed by unauthorized individuals.

**Mitigation:**
The Huron Rounding application and architecture is designed based on modern practices technology approach which includes a least access privilege model, encryption-authentication, and account control/expiration/password change. It also utilizes key encryption security approaches per the required standard. With technology vulnerability and the risk of data being compromised rising, Huron Rounding employs full transaction logging in every aspect from end user consumption/use to all backend access by Huron staff. Logging is maintained indefinitely, setup to alert and notify on out of bound conditions and reviewed on a reoccurring basis. Furthermore, Huron Rounding has annual internal and external audits and conducts vulnerability scanning and penetration testing regularly.

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.*
LEADER EVALUATION MANAGER

• Name: used to identify the user within the system
• VA Email Address: used for communications
• Department: used to group users into the department in which they work for reporting purposes
• Division: used to group users into the division in which they work for reporting purposes
• Job Title: used to specify the employee’s role within the organization
• Direct Supervisor: used to identify the individual to whom a user reports
• Hire Date: used to provide context regarding an employee’s tenure with the organization
• Goals: used to help employees reach targets stated by the organization
• Action Plans: used to demonstrate progress against individual/organizational goals

PATIENT CALL MANAGER

Patient Data:
Name: used to identify and address patient in phone communications
Date of Birth: used to identify patient
Phone Number: used to call patients
Race: used as demographic background
Medical Record Number: used to identify patient
Preferred Language: used to establish language of the phone call
Sex: used for demographic background and may help caller address the patient
Visit Number: used to reference a patient’s specific visit
Status: used to determine if patient has been discharged
Admit Date: used to ensure calls are made within proper admit/discharge timeframes
Service Date: used to ensure calls are made within proper admit/discharge timeframes
Admitting Diagnosis: may be used as part of call script
Nursing Unit Name: used to identify potential patient experience concerns
Procedure Name: may be used as part of call script
Attending Physician Name: used to escalate patient questions to provider if needed.
Patient survey responses: used to improve patient experience and provide additional information to support patient safety

Employee Data:
Name: used to identify employee using the system
Email Address: employee email address used for communication of escalated issues
Department: used to identify employee’s department within the VA
Division: used to identify employee’s department within the VA
Job Title: used to identify employee’s specific role within the VA

HURON Rounding

Huron Rounding Staff Rounding:
• Employee Name: used to tie the individual to the round
• Employee Email Address: used for communication
• Location/Department: used to group users into the department in which they work for reporting purposes
• Direct Reporting employees: used to identify direct reports who need to be rounded on
• Rounding responses: used to identify/escalate issues and improve employee engagement

Huron Rounding Patient Rounding:

• Employee Data: same as above
• Patient Data:
  o Department: used to identify department needing to round on patients
  o Facility: used to identify patient location for rounding
  o Room: used to identify patient location for rounding
  o Bed: used to identify patient location for rounding
  o Discharge Date: used to determine if patient is still in house
  o Medical Record Number: used as unique identifier for patient
  o Patient Code: may be used as unique identifier for patient
  o Patient Visit ID: used as unique identifier for patient
  o Prior Patient Code: used as unique identifier for patient
  o Prior Visit ID: used to identify if patient has previously been seen in the facility
  o Rounding responses: used to identify/escalate issues and improve patient experience

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

LEADER EVALUATION MANAGER

The Leader Evaluation Manager® (LEM) employs a weighted scoring mechanism to derive a goal score based on the leader’s performance in relation to their goals. The goal scores are utilized to drive accountability conversations with leaders and their supervisors. Reports are also available within the LEM application for visualization of goal scores and overall performance of the organization. All information within the LEM application regarding any specific leader is available to that leader and their supervisor. The goal score is intended to provide a metric of
progress towards goals and to help the leader and direct supervisor create appropriate action plans to achieve success for their goals.

PATIENT CALL MANAGER

The Patient Call Manager™ application’s primary tool for analyzing data resides in the reporting section of the tool which include patient care trends and opportunity for improvement visualization. Statistical reporting is also included to track attempt and completion rates of transition of calls made to patients.

Upon implementation Huron will work with your organization to ensure the right process are in place to support the entry of patient information into patient record appropriately.

HURON ROUNDCING

Huron Rounding’s primary tool for analyzing data resides in the reporting section of the tool which includes aggregated statistical data regarding rounding trends, such as average round duration and number of rounds completed.

Upon implementation Huron will work with your organization to ensure the right process are in place to support the entry of patient information into patient record appropriately.

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

The information system utilizes TLS1.2 for data in transit and AES-256 for data at rest. The information system does not collect or retain Social Security Numbers.

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:

LEADER EVALUATION MANAGER

VA employees needing access to the system will be determined by VA HCS leaders. Leader Evaluations will be conducted by leaders. Access will require approval and will be monitored and maintained by a system administrator, whom will be determined by VA HCS leaders in conjunction with the COR.

PATIENT CALL MANAGER

VA employees needing access to the system will be determined by VA HCS leaders. Patient calls will be conducted by VA employees. Staff members with access to the system will be responsible for safeguarding the PII. Access will require approval and will be monitored and maintained by a system administrator.

HURON ROUNDEDING

VA employees needing access to the system will be determined by VA HCS leaders. Patient rounding will be conducted by VA clinicians, and staff rounding will be conducted by HCS leaders. Staff members with access to the system will be responsible for safeguarding the PII and PHI. Access will require approval and will be monitored and maintained by a system administrator.

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.
LEADER EVALUATION MANAGER

The Leader Evaluation Manager® retains the name of leaders and their VA email address.

PATIENT CALL MANAGER

Patient Data: Medical Record Number, Preferred Language, Sex, Visit Number, Status, Admit Date, Service Date, Admitting Diagnosis, Nursing Unit Name, Procedure Name, Attending Physician Name, patient survey responses.

Employee Data: First Name, Last Name, Email Address, Department, Division, Job Title

HURON ROUNding

For patient rounding purposes, survey data is collected in the patient's room via a mobile device or computer, and data remains within the collection instrument. The unidentified data is aggregated in reports. Specific data elements maintained are: Name, Date of Birth, Email Address, Location/Department, Patient Department, Patient Facility, Room/Bed, Discharge Date, Medical Record Number, Patient Code, Patient Visit ID, Prior Patient Code, Prior Visit ID, and Patient rounding responses.

For employee rounding purposes, survey data is collected via a mobile device or computer, and data remains within the collection instrument. Specific data elements maintained are: Name, Date of Birth, Email Address, Location/Department, Direct Reporting employees, staff rounding responses, Employee Location/Department, Direct Reporting employees.

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.

LEADER EVALUATION MANAGER

Based on the SORN, the records are disposed of in accordance with General records 4.3, item 031 which states, “Destroy when superseded or obsolete, but longer retention is authorized if required for business use.”

PATIENT CALL MANAGER
Data is retained in the system for 18 months. During the Term of the Agreement, data is maintained in the live instance of Patient Call Manager for a period of 18 months and is then archived in cold storage, unless requested for reporting or access purposes by the client. Upon the conclusion of all active software services agreements with the client for such services, Huron will provide the client with the opportunity to receive an archived copy of the client data before deleting such records. Once the client confirms a copy has been received or that no copy is needed, Huron proceeds with deleting such records. Because of the possibility that the Patient Call Manager records include a unique record of patient encounters recorded by the client, Huron’s policy is to send a secure copy of such data to the client before destroying the records during the applicable retention period, unless directed by the client that no copy is needed. Pursuant to the BAA, it will be the client’s obligation to notify Huron whether to return or destroy the client’s data following the termination of our services agreement.

HURON ROUNCING

Information is retained for 7 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.

Huron was informed by the VA PIA team that the following SORNs are applicable to Leader Evaluation Manager® (LEM), Patient Call Manager™ (PCM), and Huron Rounding:

Patient Medical Records–VA (24VA10P2)
Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10)

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.

LEADER EVALUATION MANAGER
The VA will have the option of having their data returned to them at the end of the contract period, otherwise Huron will electronically destroy the data if requested. The contract states: “Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above.”

PATIENT CALL MANAGER

Electronic data including Protected Health Information (PHI) are destroyed in accordance with the Department of Veterans’ Affairs Handbook 6500.1, Electronic Media Sanitization. Hardware disposal is handled by AWS and is referenced in their SOC 1 report. In short, AWS uses techniques detailed in NIST 800-88 as part of the decommissioning process and is authorized per AWS Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO).

HURON ROUNDERING

Electronic data including Protected Health Information (PHI) are destroyed in accordance with the Department of Veterans’ Affairs Handbook 6500.1, Electronic Media Sanitization. Media disposal is handled by AWS and is referenced in their Statement of Compliance (SOC 1) report. In short, AWS uses techniques detailed in NIST 800-88 as part of the decommissioning process.

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.

LEADER EVALUATION MANAGER

The LEM utilizes very limited PII, Name and VA Email address. For testing and training, the system allows test users to be created with invented names and email addresses.
PATIENT CALL MANAGER

Artificially generated data is supplied for testing & training of Patient Call Manager™.

HURON Rounding

Artificially generated data is supplied for testing & training of Huron Rounding.

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.

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.

LEADER EVALUATION MANAGER

**Privacy Risk:** There is a risk that information be stored longer than necessary.

**Mitigation:**
The current data retention period for Leader Evaluation Manager is based on length of contract. The applicable SORN states that the data will be destroyed when suspended or obsolete, but longer retention is authorized if required for business use. Huron will provide VA with the option to accept a downloadable copy of the data so that retention requirement can be fulfilled. All data is encrypted both in transmission and at rest. Backups are maintained indefinitely and are also encrypted. A backup timeline can be adjusted if there are concerns from VA.

Customer data is purged from the Leader Evaluation Manager database at the conclusion or termination of a contract. Backup data cannot be purged but access to backups and restoration requires multiple key authentication, written approval with justification and is approved by two levels of Management.
PATIENT CALL MANAGER

**Privacy Risk:**

There is a risk that information is stored for longer than necessary.

**Mitigation:**

The current data retention period for Patient Call Manager data is 18 months. All data is encrypted both in transmission and at rest. Archived backups are maintained indefinitely and are also encrypted.

Customer data is purged from the Patient Call Manager database at the conclusion or termination of a contract. Backup data cannot be purged but access to backups and restoration requires multiple key authentication, written approval with justification and is approved by two levels of Management.

HURON ROUNDING

**Privacy Risk:**

There is a risk that information may be stored for longer than necessary.

**Mitigation:**

The current data retention period for Huron Rounding data base is seven years. All data is encrypted both in transmission and at rest. Backups are maintained indefinitely and are also encrypted.

Customer data is purged from the Huron Rounding database at the conclusion or termination of a contract. Backup data cannot be purged but access to backups and restoration requires multiple key authentication, written approval with justification and is approved by two levels of Management.

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEADER EVALUATION MANAGER</td>
<td>Contractual relationship between TVHS and Huron Consulting Services LLC</td>
<td>Personally Identifiable Information (PII)</td>
<td>Accessing LEM tool</td>
</tr>
<tr>
<td>Tennessee Valley Healthcare System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Call Manager</td>
<td>Information is received from VistA to populate the Patient Call Manager user interface.</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III)</td>
<td>Electronic: FTPS/SFTP</td>
</tr>
<tr>
<td>VistA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huron Rounding</td>
<td>Contractual relationship between TVHS and Huron</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI)</td>
<td></td>
</tr>
</tbody>
</table>
**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.

**LEADER EVALUATION MANAGER/PATIENT CALL MANAGER/HURON ROUNGING**

**Privacy Risk:**
There is a risk information could be disclosed to unauthorized internal employees.

**Mitigation:**
The Leader Evaluation Manager (LEM), Patient Call Manager (PCM), and Huron Rounding have access controls in place requiring unique assigned accounts for all authorized users of the system. There are personnel security, system and communication protection, audit and accountability, and annual awareness training controls in place. The LEM, PCM, and Huron Rounding applications and architectures are designed based on modern practices technology approach which includes a least access privilege model, encryption-authentication and account control/expiration/password change. They also utilize key encryption security approaches per the required standard. With technology vulnerability and the risk of data being compromised rising, LEM, PCM, and Huron Rounding employ full transaction logging in every aspect from end user consumption/use to all backend access by Huron staff. Logging is maintained indefinitely, setup to alert and notify on out of bound conditions and reviewed on a reoccurring basis. Furthermore, LEM, PCM, and Huron Rounding have annual internal and external audits and conducts vulnerability scanning and penetration testing regularly.

**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

<table>
<thead>
<tr>
<th>Data Shared with External Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>List External Program Office or IT System information is shared/received with</strong></td>
</tr>
<tr>
<td>LEADER EVALUATION MANAGER</td>
</tr>
<tr>
<td>Huron Consulting Services LLC</td>
</tr>
<tr>
<td>Patient Call Manager</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Huron Rounding</td>
</tr>
</tbody>
</table>

Huron
Consulting
Services LLC

Data is housed on Huron’s servers

Medical Record Number, Preferred Language, Race, Date of Birth, Sex, First Name, Last Name, Home Phone, Visit Number, Status, Admit Date, Service Date, Admitting Diagnosis, Nursing Unit Name, Procedure Name, Attending Physician Name, patient survey responses

Business Associate Agreement, MOU-ISA in process

SFTP/FTPS in compliance of FIPS 140 – 2 for encrypted storage and transmission of all PII/PHI.
LEADER EVALUATION MANAGER

Administrative, technical, and physical safeguards have been implemented to protect sensitive data. These controls include: logs of all interactions with sensitive data, use of VPN to ensure proper authentication and security, and policies, procedures, and training as required by FEDRAMP low classification. Use of mobile devices is not supported by Leader Evaluation Manager™.

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

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.

LEADER EVALUATION MANAGER/PATIENT CALL MANAGER/HURON Rounding

Privacy Risk:
There is a risk that information could be shared with unauthorized external individuals.

Mitigation:
The Leader Evaluation Manager (LEM), Patient Call Manager (PCM), and Huron Rounding have access controls in place requiring unique assigned accounts for all authorized users of the system. There are personnel security, system and communication protection, audit and accountability, and annual awareness training controls in place. The LEM, PCM, and Huron Rounding applications and architectures are designed based on modern practices technology approach which includes a least access privilege model, encryption-authentication and account control/expiration/password change. They also utilize key encryption security approaches per the
required standard. With technology vulnerability and the risk of data being compromised rising, LEM, PCM, and Huron Rounding employ full transaction logging in every aspect from end user consumption/use to all backend access by Huron staff. Logging is maintained indefinitely, setup to alert and notify on out of bound conditions and reviewed on a reoccurring basis. Furthermore, LEM, PCM, and Huron Rounding have annual internal and external audits and conducts vulnerability scanning and penetration testing regularly.

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.

LEADER EVALUATION MANAGER

Huron Consulting Services posts a copy of the Huron Privacy Statement on its website in order to notify users of the Huron Consulting Services’ websites and other services that their information is being collected and used appropriately (https://www.huronconsultinggroup.com/legal/privacy-policy). At this time, a separate link to the Huron Privacy Statement is not included within the online portal for the Leader Evaluation Manager software application but will be added in a future update to the system. This PIA also serves as a form of notice. The Huron Privacy statement will be included in training materials distributed to Administrators prior to launch.
Since VA leaders will be using LEM to record information about themselves in their capacity as employees of the TVHS, the Department of Veterans Affairs National Rules of Behavior for employees applies.

PATIENT CALL MANAGER

Huron Consulting Services posts a copy of the Huron Privacy Statement on its website in order to notify users of the Huron Consulting Services’ websites and other services that their information is being collected and used appropriately (https://www.huronconsultinggroup.com/legal/privacy-policy). At this time, a separate link to the Huron Privacy Statement is not included within the online portal for the Patient Call Manager software application.

For purposes of PCM, patient information is collected in accordance with the VHA Notice of Privacy Practices IB 10-163 in accordance with VA’s Notice of Privacy Practices, which is set forth in VHA Handbook 1605.04. To support the education of staff members on the tool, example language can be provided to staff to inform individuals that information is being collected during the call and will be used to support the patient post-discharge.

HURON ROUNding

Huron Consulting Services posts a copy of the Huron Privacy Statement on its website in order to notify users of the Huron Consulting Services’ websites and other services that their information is being collected and used appropriately (https://www.huronconsultinggroup.com/legal/privacy-policy). At this time, a separate link to the Huron Privacy Statement is not included within the online portal for the Huron Rounding software application.

Terms and conditions may be viewed from Huron Rounding in a couple ways:
1. Within the footer of the marketing website (www.Huron Rounding.com). This links directly to https://www.huronconsultinggroup.com/legal/terms-and-conditions

For purposes of Huron Rounding, patient information is collected in accordance with the VHA Notice of Privacy Practices IB 10-163 in accordance with VA’s Notice of Privacy Practices, which is set forth in VHA Handbook 1605.04. To support the education of staff members conducting rounds, example language can be provided to staff to inform individuals that information is being collected during the rounding conversation and will be used to improve future patient experience or employee engagement, as applicable.

Huron was informed by the VA PIA team that the following SORNs are applicable to Leader Evaluation Manager (LEM), Patient Call Manager (PCM), and Huron Rounding:
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.

LEADER EVALUATION MANAGER

Individuals will have the opportunity to control the information provided, subject to VA’s policies for opting out of annual performance review processes.

PATIENT CALL MANAGER

Information will be collected and stored in PCM directly by employees and other representatives of the Tennessee Valley Healthcare System. The Tennessee Valley Healthcare System will have control over what information to collect and from whom. Pursuant to VHA Notice of Privacy Practices IB 10-163, no authorization will be needed from the person whose information is collected to the extent used for purposes of improving the Tennessee Valley VA Healthcare System Care Operations.

HURON ROUNDING

Information will be collected and stored in Huron Rounding directly by employees and other representatives of the Tennessee Valley Healthcare System. The Tennessee Valley Healthcare System will have control over what information to collect and from whom. Pursuant to VHA Notice of Privacy Practices IB 10-163, no authorization will be needed from the person whose information is collected to the extent used for purposes of improving the Tennessee Valley VA Health Care Operations. However, individuals do have the opportunity to decline at the time of rounding.

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.
LEADER EVALUATION MANAGER

For the Leader Evaluation Manager®, consent is given to cover all uses of his or her information.

PATIENT CALL MANAGER

Per VHA Notice of Privacy Practices IB 10-163, no individual consent is required for those specific uses outlined in the Notice. Other uses will require the authorization of the individual whose information has been collected in accordance with the terms of the Notice.

HURON ROUNDING

Individuals are asked to provide their PII at the time it is entered in this system and have an opportunity to object to the specific uses of their PII. If they choose not to consent to the specific uses of their PII, comprehensive health care services may not be possible, they may experience administrative delays, and they may be rejected for service or an assignment. However, care will not be denied.

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

LEADER EVALUATION MANAGER

Risk: There is a risk that individuals are unaware that their information is being collected.

Mitigation: For the Leader Evaluation Manager®, each user’s consent is given to cover all uses of his or her information.

PATIENT CALL MANAGER

Risk: There is a risk that individuals are unaware that their information is being collected.
Mitigation: Per VHA Notice of Privacy Practices IB 10-163, no individual consent is required for those specific uses outlined in the Notice. Other uses will require the authorization of the individual whose information has been collected in accordance with the terms of the Notice.

HURON ROUNDING

Risk: There is a risk that individuals are unaware that their information is being collected.

Mitigation: Individuals are asked to provide their PII at the time it is entered in this system and have an opportunity to object to the specific uses of their PII. If they choose not to consent to the specific uses of their PII, comprehensive health care services may not be possible, they may experience administrative delays, and they may be rejected for service or an assignment. However, care will not be denied.

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.

LEADER EVALUATION MANAGER

Individuals with LEM accounts may access their information at any time utilizing a web browser to access the LEM tool.

PATIENT CALL MANAGER
PCM receives an automated daily data extract from VistA, containing records of recently discharged patients, that is ingested into the PCM application. Therefore, patients may make updates to their demographic data in person, or in writing, to the Business Office. Patients may request an amendment of any medical record by submitting a written request to the VA Privacy Officer. An amendment request will be processed per the guidance in VHA Directive 1605.01 (Privacy and Release of Information). Those updates will be transmitted to PCM. Individual patients should look at the PIA for their specific HCS/VAMC for more information.

Additionally, information is collected from individuals during post-discharge calls. Individuals may work with the VA, who owns the data, to access information stored in the system.

**HURON ROUNding**

Data elements are manually input into VistA. As stated in Huron’s Business Associate Agreement, the VA has control over deciding how to respond to individuals’ requests for amendment and that Huron will take action only as instructed by VA in accordance with the terms of our Business Associate Agreement.

Regarding staff rounding, employees will be emailed a copy of the round to ensure notes were captured correctly. Should a completed round need to be modified the submitter or assigned Content Admin can modify the content for 30 days post submission. The initial round date cannot be modified, and all changes are tracked and logged but cannot be seen from the front-end Huron Rounding application.

### 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.

**Leader Evaluation Manager**

Individuals have the opportunity to correct information they have submitted within the LEM tool. Leaders may work with their supervisors to revise goals or progress notes regarding goals that have been entered incorrectly.

**Patient Call Manager**

Patients may correct demographic data in person, or in writing, through the Business Office and submit a written request to the Privacy Officer for the correction of any medical record. An amendment request will be processed per the guidance in VHA Directive 1605.01 (Privacy and Release of Information). Any updates made in the VistA medical record will be automatically transmitted to PCM. As stated in Huron’s Business Associate Agreement, the VA has control over deciding how to respond to individuals’ requests for amendment and that Huron will take action only as instructed by VA in accordance with the terms of our Business Associate Agreement.
HURON Rounding

Updates to data stored within the Rounding application will require manual entry and correction by VA end users. As the Rounding application does not receive an automated data extract from VistA, changes made in VistA will not be automatically reflected in the Rounding application. As stated in Huron’s Business Associate Agreement, the VA has control over deciding how to respond to individuals' requests for amendment and that Huron will take action only as instructed by VA in accordance with the terms of our Business Associate Agreement.

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.

Leader Evaluation Manager

Huron will provide training to leaders on how to use the tool, including updating of personal information.

Patient Call Manager

Because the administration and management of patient information will be the responsibility of the TVHS VA, Individuals will be notified of procedures for correcting their medical record using established VA communication mechanisms.

Huron Rounding

Individuals are notified of procedures for correcting their medical record using the guidance in the VistA PIA for their facility.

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.

LEADER EVALUATION MANAGER

Users can directly access their information and correct and update it via the LEM software.

PATIENT CALL MANAGER

N/A

HURON ROUNding

N/A

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.

LEADER EVALUATION MANAGER

Follow the format below:

Privacy Risk:
There is a risk that individuals will be unaware as to how they can correct inaccurate or erroneous information.

Mitigation:
The Leader Evaluation Manager supports correction to information inaccurately documented in the Evaluation. The Leader Evaluation Manager training guide and help section provide detailed instructions to allow individuals direct access to revise their information or edit and correct inaccurate information.

PATIENT CALL MANAGER

**Privacy Risk:**

There is a risk that individuals will be unaware as to how they can correct inaccurate or erroneous information.

**Mitigation:**

The Patient Call Manager application supports redress & correction to information inaccurately documented during a call. The Patient Call Manager™ training guide and help section provide detailed instructions for completing correction tasks within the Patient Call Manager application that may be followed directly by the VA end users. Because the Patient Call Manager application pulls data directly from VistA, individuals should follow the steps listed in their HCS/VAMC facility’s PIA to correct any inaccurate or erroneous information. Pursuant to our Business Associate Agreement with the Veterans Health Administration, Huron will defer to the instructions of VA/TVHS with respect to requests to amend individual patient records.

HURON ROUNDING

**Privacy Risk:**

There is a risk that the content admin/round submitter is unaware of how to access or correct inaccurate information.

**Mitigation:**

The Huron Rounding application allows a Round submitter or assigned Content Admin to modify the content or a completed Round. Should a completed Round need to be modified, the submitter or assigned Content Admin can modify the content for 30 days post submission. The initial Round date cannot be modified and all changes are tracked and logged but cannot be seen from the front end Huron Rounding application. Individuals (other than VA end users and administrators) cannot gain direct access to the Huron Rounding application to make corrections directly. Pursuant to our Business Associate Agreement with the Veterans Health Administration, Huron will defer to the instructions of VA/TVHS with respect to requests to amend individual patient records.

**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.

LEADER EVALUATION MANAGER

Individuals receive access based on the recommendation of the VA Medical Center’s leadership team. Upon receipt of recommended users, the Huron team will provide login credentials to each individual. Users access the system using login and passwords that are unique to each user. LEM also has single-sign on capability, which would allow users to login with their VA-provided system credentials. (q) The LEM system contains 3 role types with access as described below.

OrgAdmin: System Administrator with read/write/delete authority to create, modify, or edit user accounts.

LEM Admin: LEM tool administrator with read/write/delete authority for entire LEM system.

LEM User: Read/Write/Delete authority only for user’s evaluation, goals, and action plans. In all other areas of LEM, the LEM user is read-only.

PATIENT CALL MANAGER

Individuals receive access based on the recommendation of the VA Medical Center’s leadership team. Upon receipt of recommended users, the Huron team will provide login credentials to each individual. Users access the system using login and passwords that are unique to each user. PCM also has single-sign on capability, which would allow users to login with their VA-provided system credentials.

HURON ROUNDING

Individuals (VA employees and contractors) receive access based on the recommendation of the VA Medical Center’s leadership team. Upon receipt of recommended users, the Huron team will provide login credentials to each individual. Users access the system using login and passwords that are unique to each user. Huron Rounding also has single-sign on capability, which would allow users to login with their VA-provided system credentials.
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.

LEADER EVALUATION MANAGER

Yes, the Leader Evaluation Manager system is developed and maintained by contractors. Design and maintenance will be exclusively handled by Huron Consulting Services LLC. Contractors will need access to PII to properly maintain the system and train new users.

PATIENT CALL MANAGER

Yes, the Patient Call Manager system is developed and maintained by Huron Consulting Services LLC, a VA contractor. No additional subcontractors have access to the system. Design and maintenance will be exclusively handled by Huron Consulting Services LLC. A national Business Associate Agreement is in place between VHA and Huron Consulting Services LLC. Contractors will need access to PII to properly maintain the system and train new users.

HURON Rounding

Yes, the Huron Rounding system is developed and maintained by Huron Consulting Services LLC, a VA contractor. No additional contractors of Huron Consulting Services will have access to live system data. Design and maintenance will be exclusively handled by Huron Consulting Services LLC. A national Business Associate Agreement is in place between VHA and Huron Consulting Services LLC. Contractors will need access to PII to properly maintain the system and train new users.

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.

LEADER EVALUATION MANAGER
Huron Consulting Services staff who have access to this system have completed VA Privacy and Security training courses. It is the VA’s responsibility to provide appropriate training to its staff, and it is assumed that VA staff using this system have completed the requisite privacy training as well.

PATIENT CALL MANAGER

Huron Consulting Services staff who have access to this system have completed VA Privacy and Security training courses. It is the VA’s responsibility to provide appropriate training to its staff, and it is assumed that VA staff using this system have completed the requisite privacy training as well.

HURON ROUNCING

Huron Consulting Services staff who have access to this system have completed VA Privacy and HIPAA and Information Security/Contractor Rules of Behavior training courses. It is the VA’s responsibility to provide appropriate training to its staff, and it is assumed that VA staff using this system have completed the requisite privacy training as well.

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.

LEADER EVALUATION MANAGER

Authority to Operate has not yet been granted.
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.

The information system utilizes AWS GovCloud. Huron is currently seeking FedRAMP ATO approval for the Huron Accelerators Platform (HAP) which consists of Leader Evaluation Manager, Patient Call Manager, Huron Rounding. HAP is the name of the system that TVHS VA will be installing and using.

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.

AWS GovCloud
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.

The contract (#36C24918C0193) includes language, including without limitation Section B.4, relating to data rights between the parties and related security controls, and also incorporates a Software as a Service Agreement, which provides: Section 2.3 (Proprietary Rights) establishes Service Provider’s ownership of the Services, the Service Provider Data (excluding any Client Content included therein), and any modifications, configurations, enhancements or derivative works thereof. Section 3.1 of the Software as a Service Agreement defines “Client Content” as any information or data related to Client that is input into the SaaS Service or provided by Client to Service Provider (Huron) for entry by Service Provider into the SaaS Service pursuant to a SOW. Therefore, Service Provider has expressly excluded the Client Content from the ownership rights Service Provider assets to data under the contract. Other relevant provisions of the Software as a Service Agreement include: (a) Section 3.2, which states that any PHI shall be protected under the applicable business associate agreement*;(b) Section 3.3, which provides that PII may only be used by Service Provider for purposes of the Agreement and as directed by Client; (c) Section 3.4, which defines “Service Provider Data” as data collected by Service Provider arising out of Client’s use of the SaaS Services; metrics and data included in the Client Content; and aggregations or analysis of such metrics or data; provided, that it is de-identified to exclude any PHI and does not identify Client as the source of any data; and (d) Section 3.5, which confirms that Client Content is the Confidential Information of Client, while Service Provider Data is the Confidential Information of Service Provider. Although not expressly stated in the contract, Service Provider has interpreted the exclusion of Client Content in Section 2.3 and the classification of Client Content as the Confidential Information of Client under Section 3.5 as confirmation of the government’s retained ownership over the Client Content, which would include any PII Client includes in our software applications. * Further, the “Terms and Conditions” section of the Business Associate Agreement between Service Provider and Veterans Health Administration establishes Tennessee Valley Healthcare System’s ownership of all PHI provided by Tennessee Valley Healthcare System as the Covered Entity to Service Provider as Business Associate under the Agreement.

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.

Yes, ancillary data is collected in accordance with the terms of the contract (#36C24918C0193), including the Software as a Service Agreement incorporated into the contract as Attachment D. Except to the extent inapplicable with federal procurement law and specifically excluding any PHI/PII or other government content, the Software as a Service Agreement grants Contractor as service provider ownership rights over the ancillary data.

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.

The contract (#36C24918C0193) includes language holding Contractor directly accountable for the security and privacy of data held under the contract, regardless whether a cloud provider is used to host the data on Contractor’s behalf. Contractor will be responsible for paying the government liquidated damages in the event of a data breach and will be responsible for conducting annual self-assessments and ensuring that the included services meet the security and privacy requirements of the contract and Applicable Law.

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).

The solution does not utilize Robotic Process Automation.
### Section 9. References

**Summary of Privacy Controls by Family**

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

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

ROBBIE BRASWELL
Digitally signed by ROBBIE BRASWELL
Date: 2021.10.28 13:35:32 -05'00'

Privacy Officer, Robbie Braswell

ANDREW VILAILACK 1811006
Digitally signed by ANDREW VILAILACK 1811006
Date: 2021.11.01 07:10:03 -04'00'

Information System Security Officer, Andrew Vilailack

FRED TOLLEY
Digitally signed by FRED TOLLEY
Date: 2021.11.01 08:27:04 -04'00'

System Owner, Fred Tolley
Privacy Statement

Huron Consulting Group Inc. and its subsidiaries: Huron Consulting Services LLC; Huron Advisors Canada Limited; Huron Eurasia India Private Limited; Huron Managed Services LLC; Huron Transaction Advisory LLC; Innosight Consulting, LLC; Innosight Consulting Asia-Pacific Pte. Ltd; Innosight Consulting SARL; Pope Woodhead and Associates Limited; and, The Studer Group, L.L.C. (“Huron” or “we” or “our” or “us”) are committed to protecting your privacy when you interact with us.

This Privacy Statement (“Privacy Statement or “Statement”) sets out the privacy practices for Huron with respect to Personal Data and Personal Information (which means any information that relates to, identifies, describes, or can be reasonably associated or linked with a natural person or household) we obtain from and about individuals interacting with Huron and its websites, mobile applications, and services. All Personal Data that we collect, other than information collected in the employment context, is subject to this Privacy Statement.

Please read the information below to learn about the Personal Data collected about you and how it is used. Please note that there is a separate Terms of Use found in the “Terms & Conditions” hyperlink located at the bottom of our website. We may revise this Privacy Statement from time to time and will do so by posting additions or modifications to this page. The most current version of the Statement can always be reviewed by clicking on the “Privacy Statement” link located at the bottom of our website.

If you are a resident of California, please see the section below titled, “Additional Information for Residents of California.”

If you are located in the European Union (“EU”), United Kingdom (“UK”), Switzerland, or where applicable EU data protection laws so provide, please see the section below titled, “Additional Information for Individuals Located in Europe.”.

Contact information

Event registrations and preferences

Feedback and reviews or request for support
Log files, information collected by cookies and similar technologies about the pages viewed, links clicked and other actions taken when accessing our website, which may be considered Personal Data under applicable laws (see our Cookie Policy for more information).

Resumes and information relevant to our market research activities that: you provide to us directly; we receive about you from referrals; or we collect from publicly available sources and websites.

If you are being considered for employment with Huron, we may collect and process the following types of Personal Data:

Resume, application, candidate profile, or interview logistics information during the recruiting process. The sources of employment application information include yourself (when you provide information directly to us, for example, through our job postings portal on this website), publicly available information (such as information on job posting websites), and external recruiting sources (such as professional recruiting or placement agencies).

Huron also collects Personal Data from other Huron entities (including those listed at the beginning of this Statement). In addition, Huron may collect Personal Data from service providers who provide services to us, such as web analytics providers.

Huron collects and uses Personal Data for our legitimate interests as set out herein, or based on your consent (in which case we would ask you separately to provide your consent to a particular processing activity) through:

Personalizing your experience on our website, such as providing recommendations based on your industry or past behavior on the website.

Providing services, training and education, tools (such as Huron Software accelerators), products (such as books), and support to our customers, which may also be necessary for the performance of a contract with you.

Conducting business with our suppliers and other entities, including market research activities.

Considering candidates for job vacancies with Huron entities, including all elements of the procedure leading up to making a decision whether to offer, subject to any appropriate...
background checks, the applicant a position. Some job applicant data processing may also be necessary to comply with legal obligations.

In instances where information is transferred to Huron through a client data controller and Huron is acting as the processor, the processing is necessary for the performance of a contract or for our legitimate interest to provide the requested services to our clients. Huron will assist the client data controller in complying with its legal obligations, discussed below in the Additional Information for Individuals Located in Europe section, where applicable.

With Whom We Share Personal Data

Huron may share Personal Data we collect with the following entities and for the following purposes:

Subsidiaries who process Personal Data on behalf of Huron for the purposes of supporting and providing services to our customers

Service providers contracted to provide services on behalf of Huron for discrete business purposes such as provision of IT related services, event planning, talent recruiting, market research interviewees and providers, and travel services

Entities with whom Huron works in providing a service, such as educational establishments with whom Huron collaborates to provide training and certification, and organizations at which Huron arranges for students to obtain practical experience

Retention of Data

We will keep your Personal Data as reasonably necessary to fulfill the purposes for which Personal Data is collected as stated herein; for as long as is necessary for the performance of the contract between you and us, if any; and to comply with legal and statutory obligations, such as those required by tax, trade and corporate laws. When we no longer need your Personal Data for our purposes, we will destroy, delete or erase that Personal Data or convert it into an anonymous form.

If you have questions, complaints or concerns regarding this Privacy Statement or wish to access your Personal Data, or update, change or remove your Personal Data, please contact privacy@huronconsultinggroup.com, or send mail addressed to:
Huron Consulting Group Inc.
Attn: Chief Privacy Officer
550 W Van Buren St, Chicago IL 60607

This website is not intended for children under the age of 13. We will not knowingly collect information from website visitors in this age group. By using the Site, you represent that you are age 13 or over. If you believe that a child may have provided his or her Personal Data to us, please contact us using the contact information at the end of this Statement. In the event we become aware that we have collected Personal Data from a child under the age of 13, we will dispose of that Personal Data immediately.

Additional Information for California and Europe

Contact Us

We have taken great measures to ensure that your visit to our website and your interactions with Huron are satisfying and that your privacy is respected. Unless otherwise stated, Huron is a business and data controller for Personal Data processed subject to this Statement. Because Huron is a professional services firm focused primarily on serving other businesses, Huron is a service provider and data processor to our clients for Personal Data that belongs to the data subjects and consumers who are associated with those clients. If you have any questions, comments or concerns about our privacy practices, please contact us by e-mail at privacy@huronconsultinggroup.com.

Copyright 2012-2020 Huron Consulting Group Inc. and its subsidiaries

Effective as of October 2020