Centers for Medicare & Medicaid Services

Patient Protection Affordable Care Act (ACA)
Enhanced Direct Enrollment Entity

Privacy Impact Assessment (PIA) Form

Version 1.0

February 13, 2018

Foreword

The Centers for Medicare & Medicaid Services (CMS), the Center for Consumer Information and Insurance Oversight (CCIIO), in collaboration with the Office of Information Technology (OIT), have developed this Privacy Impact Assessment (PIA) form. The intent of the PIA is to complement the descriptions of privacy controls in the System Security Plan (SSP) by assisting Non-Exchange Entities (NEEs) in assessing compliance with applicable legal, regulatory, and policy requirements and accounting for the NEE's privacy program and information systems that collect, use, disclose, and/or retain Personally Identifiable Information (PII).

Should you have any questions about this PIA form, please submit your questions to the CMS ACA Security and Privacy Mailbox at ACASecurityandPrivacy@cms.hhs.gov.

The use of this form is strongly recommended for all new and updated PIAs conducted by the NEEs.

Record of Changes/Change History Table

Update the following table to document and track changes made to the PIA.

Version Number	Version Date	Author/Owner	Summary of Change(s)

The Non-Exchange Entity privacy official responsible for the oversight and monitoring of the Non-Exchange Entity's privacy program or their designee must approve and sign the PIA. CMS will only accept PIAs signed by the Non-Exchange Entity's privacy official or their authorized designee.

Name _____

(Non-Exchange Entity Privacy Official or Authorized Signatory)

Title _____

Signature _____

Date _____

Table of Contents

Purpose and Intended Use of the PIA

[AR-2]

The Privacy Impact Assessment (PIA) is designed to help the Non-Exchange Entity (NEE) identify the specific types of sensitive information it will collect, process, and store while participating in the Open Enrollment; assess privacy risks associated with maintaining that information; and subsequently document the risk assessment results. The PIA must be completed by NEEs that are participating in Open Enrollment. It is the responsibility of the NEE to ensure the privacy of individuals and to protect their Personally Identifiable Information (PII)[1] and Protected Health Information (PHI).[2] (**Note:** PHI is a subset of PII. Anything that applies to PII also applies to PHI, but not vice versa.) This PIA focuses on PII, not PHI, and is not intended to assess compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Section 1311 of the ACA and Health and Human Services (HHS) ACA Regulation § 155.280 provides authority for CMS oversight.

The PIA is one of the required compliance artifacts within the Business Agreement. The PIA is intended to demonstrate the NEE environment in which PII will be collected, used, disclosed, and/or retained. Together with the System Security Plan (SSP), the PIA will help synchronize the privacy and security efforts of both the NEE and the federal government and, as such, must at a minimum be completed annually or when significant changes occur related to the collection, use, disclosure, and/or retention of PII.

An independent third-party assessor will use the responses provided within the PIA and subsequent discussions with NEE privacy representatives to understand how the NEE has interpreted and implemented the privacy obligations within 45 CFR §155.260. (**Note:** Other federal, state, or territory privacy laws and regulations may also apply to the NEE in addition to 45 CFR §155.260. The PIA is not designed to evaluate compliance with any other applicable privacy laws and regulations. It is the NEE's responsibility to ensure compliance with all applicable privacy laws and regulations.)

[1] PII is defined by Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017). PII means information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual.

[2] PHI is any health information, including demographic information, that relates to an individual's physical or mental health and the provision of or payment of health care, and that identities the individual.

Instructions for Completion

1. Ensure the most current PIA form is used (February 2018, Version 1.0).
2. Ensure responses are typed in Times New Roman font, font size 12, and left justified.
3. Do not change or modify the form or delete any questions.
4. Ensure that all questions are answered completely, including marking applicable check boxes.
5. If the question is not applicable, indicate so and explain why.
6. Ensure all acronyms are spelled out on first use.
7. Ensure that responses to the PIA are consistent with the relevant information in the SSP.
8. Ensure all PII data elements used are referenced in this PIA. Conventional aggregations of elements may be used, such as “address” in lieu of “street name, city, state, zip code”.
9. Ensure the names of all systems provided in the SSP are also identified in the PIA and that the names are consistent.
10. Ensure the final PIA is reviewed, validated, signed, and dated by the Non-Exchange Entity’s privacy official.
11. Delete this instruction page and all sections with blue text from your final version of this document.

1. General/Administrative Information

The following entries address general and administrative information regarding the Non-Exchange Entity.

1.1 NEE Partner Name

Provide the name of the NEE.

[Click **here** and type text here]

1.2 Privacy Overview and Program POC

Identify the individual responsible for the oversight and monitoring of the NEE's privacy program.

Privacy Overview and Program POC Data	Response
Name:	
Title:	
Organization:	
Email:	
Phone Number:	

1.3 System Name

Provide the name of the system(s) the NEE currently uses or intends to use to perform the NEE functions.

[Click **here** and type text here]

2. Privacy Program Assessment

[AR-1]

The following entries in this section addresses aspects of the NEE Partner's privacy program.

2.1 Roles and Responsibilities

Describe the roles and responsibilities associated with individuals responsible for the implementation and maintenance of all aspects of the organization's privacy program.

These individuals include, but are not limited to, the senior privacy official, business owners, security and privacy officers, privacy official responsible for reviewing and approving PIAs, legal POC, system developers, training officials, and records management staff. Also, describe any mechanisms (e.g., cross-functional committees or working groups) intended to coordinate these responsibilities across roles.

Privacy risk factors include, but are not limited to:

- Individuals splitting time between multiple roles
- Insufficient horizontal and/or vertical coordination mechanisms

[Click **here** and type text here]

2.2 Dissemination of Privacy Program Information (Policy, Procedures, Standards, Guidelines)

[TR-3]

Describe how privacy guidance documents, including specific policies, procedures, and standards governing the implementation and maintenance of the privacy program, are disseminated once they are developed, including how they are communicated within the organization and to other external stakeholders, including the public.

Privacy risk factors include, but are not limited to:

- Unreliable mechanisms for alerting stakeholders to changes in guidance or access procedures
- Insufficient cross-referencing between topical information and roles and responsibilities

[Click **here** and type text here]

2.3 Legal Compliance

[AP-1]

Describe how the organization monitors compliance with federal statutes, state laws, and regulations governing the collection, use, maintenance and sharing of PII (e.g., training on these

organizational authorities for collecting PII, or periodic reviews of these documented legal authorities against the organizational purpose for collecting PII).

These legal authorities must be clearly documented. Describe how these authorities relate to the program and system purpose.

Privacy risk factors include, but are not limited to:

- Insufficiently comprehensive or frequent reviews of legal requirements
- Unreliable monitoring mechanisms for notification of legal changes
- Ambiguous procedures for responding to changes in legal requirements

[Click **here** and type text here]

2.4 Incident Handling

[SE-2]

The entries in this subsection focuses on how privacy incidents are identified, investigated, reported, and communicated to individuals within the organization and to external stakeholders.

2.4.1 Investigation

Describe how privacy incidents are investigated, including security aspects, and how frequently the investigation processes are tested.

This description should identify the individuals (e.g., privacy officer, chief compliance officer, security officer) within the organization who are responsible for providing oversight for any aspect of incident management. Being prepared to respond to and mitigate incidents is critical to the success of a privacy program.

Privacy risk factors include, but are not limited to:

- Ambiguous mapping of roles to procedures
- Insufficient provision for post-mortem analysis and process improvement
- Insufficient process tests or exercises

[Click **here** and type text here]

2.4.2 CMS Notification

Describe the process of how suspected and known privacy incidents will be reported to CMS, including who is responsible for making the notification.

Note: According to IR-6 and SE-2, NEEs are required to report any security and privacy Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour after discovery of the Incident or Breach.

This response should detail how the NEE will report all suspected and known incidents to CMS within the required timeframe. The response should identify who (e.g., privacy officer, chief compliance officer) within the organization is required to provide notification to CMS.

Privacy risk factors include, but are not limited to:

- Insufficiently defined lines of authority and designated alternates for notification decisions and actions
- Unreliable contact mechanisms
- Limited dissemination of contact information of responsible roles/individuals

[Click **here** and type text here]

2.4.3 Individual Notification

Describe the process that will determine when individuals affected by a suspected or confirmed privacy incident, within and outside of the organization, will be notified and the means of notification.

Privacy risk factors include, but are not limited to:

- Insufficiently defined lines of authority and designated alternates for notification decisions and actions
- Insufficient pre-arranged notification capability, including diversity of mechanisms
- Ambiguous decision process or framework

[Click **here** and type text here]

2.5 Training

[AR-5]

The entries in the following subsections are designed to determine organizational compliance with privacy controls through the effective implementation and use of specific methods for privacy and security training and awareness. These methods of training include providing role specific training for individuals with significant information security and privacy responsibilities and ensuring all employees and contractors are aware of and acknowledge compliance with privacy and security requirements.

2.5.1 Role-Based Privacy Training

Describe how employees and contractors with significant privacy and security responsibilities are provided with role-specific training, which should include security and privacy safeguards.

These specific roles include system, network and database administrators, auditors, and privacy officers. The response should indicate for each role, the types of training received, the frequency of training, and a summary of the content of that training.

Privacy risk factors include, but are not limited to:

- Insufficient role specificity or differentiation
- Insufficient training reviews and updates

[Click **here** and type text here]

2.5.2 Rules of Behavior

Describe the documented privacy and security related rules of behavior, or any other types of agreements, that apply to all system users (e.g. employees and contractors) that they are required to review and abide by. Include how often these rules and/or agreements are required to be reviewed.

Privacy risk factors include, but are not limited to:

- Insufficiently frequent reviews of the rules of behavior
- Insufficiently flexible sanctions, creating reluctance to impose sanctions

[Click **here** and type text here]

2.5.3 Acknowledgement

Describe the process and its frequency for ensuring employees and contractors formally acknowledge that they understand and agree to abide by the constraints (e.g., documented in rules of behavior) associated with the privacy and security programs and information systems maintaining PII.

Privacy risk factors include, but are not limited to:

- Insufficient tracking of acknowledgements
- Insufficiently frequent acknowledgements
- Isolation of acknowledgment from rules of behavior

[Click **here** and type text here]

2.6 Risk Management

Describe the process or methodology in place to identify and assess privacy risks to business processes and individuals resulting from the collection, use, disclosure, and/or retention of PII.

The response should describe the NEE's risk management process, how privacy risks are identified, and the methods in place to mitigate those risks. Indicate how this is applied to organizational life cycle processes, including system development.

Privacy risk factors include, but are not limited to:

- Insufficient integration of risk management into life cycle processes, including maintenance

- Ambiguously defined responsibilities for privacy risk management activities
- Insufficiently frequent review and updating of privacy risk management processes
- Insufficient tool support for privacy risk management processes

[Click **here** and type text here]

2.7 Assessment of Risk

Complete the table below to describe the risk factors identified in Sections 1 and 2. This will assist in determining risks and gauging their potential impact on the organization and individuals. Noncompliance with a required control is by definition a risk factor and should be noted in the table below. Compensating controls are acceptable when circumstances prevent directly mitigating the risk factor or as a temporary measure while directly applicable controls are in the process of being implemented. Compensating controls must be clearly explained and justified. Decisions can then be made regarding requirements to mitigate the risks of collecting, using, maintaining, and disseminating PII. Delete the examples from the final version of this document.

Applicable Risk Factor	Potential Impact of Risk Factor	Compensating Controls and Justification	Additional Planned Controls
Example: No specific privacy POCs in place	Inability to determine privacy requirements required to be in place to protect individuals and/or the organization	Security POC currently in place with knowledge of privacy requirements	Role-based privacy and security training scheduled to be in place within the month.
Example: Lack of a documented incident response plan	Potential inadvertent exposure of PII data with no accountability	During privacy awareness for all users, training is provided on privacy breaches and how to report them.	An incident response plan will be developed within the next three weeks which will include documented breach notification procedures.

3. System Assessment

This set of entries are intended to evaluate privacy-related properties of the system.

Note: The term "system" refers to all business processes and technical components that implement NEE Partner functions.

3.1 System Changes since Last Submission

Describe any changes to the system since the last PIA submission that relate to the creation, collection, use, disclosure, and/or retention of PII.

Any changes to business processes or information technology that affect how PII is handled should be described. These can include, but are not limited to:

- Deploying new information technology or making changes to existing information technology
- Modifying the Non-Exchange Entity functions
- Transitioning to another Marketplace model
- Modifying access requirements for staff and contractors
- Creating, collecting, using, or disclosing new PII elements
- Using or disclosing PII for new purposes
- Working with new third-party entities or terminating relationships with existing ones
- Modifying data sharing agreements

[Click **here** and type text here]

3.2 Outsourcing and Offshoring

Outsourcing involves contracting with a third-party entity (i.e., a vendor or service provider) who will have access to system PII within the U.S. Offshoring involves contracting with a third-party entity (i.e., a vendor or service provider) who will have access to system PII outside the U.S. Access can include the following functions: collection, use, disclosure, and/or retention. Privacy risk can arise any time an organization relinquishes direct control over PII, particularly in the case of offshoring, where distinctly different legal requirements and standards of practice may normally prevail.

Privacy risk factors include, but are not limited to:

- Insufficiently comprehensive or frequent vendor privacy and security assessments
- Insufficient legal analysis (out-of-state and out-of-country)
- Insufficient vendor auditing provisions

Specify whether the system, in support of any of its functions, outsources or offshores PII.

Does a vendor or service provider have access to system PII within the U.S. (outsourcing)?

Yes: ___ No: ___

Does a vendor or service provider have access to system PII outside the U.S. (offshoring)?

Yes: ___ No: ___

3.3 System Description

[AP-1, AP-2, AR-7]

The following entries in this subsection involves mapping system operations to applicable functions as described in subsections 3.3.1 – 3.3.2.

The system description should enable the reviewer to understand how the system carries out each relevant function by describing what PII the system takes from where and how, how it processes it, and what PII goes where and how as a result. This is not intended to imply that system operations can or must be described in a purely three-step linear fashion; however, operations should be explicitly described in terms of these basic elements. Once initially described, system components with specific names or designations can simply be referenced in the descriptions for later functions; it is not necessary to replicate identical component descriptions. This also applies to any diagrams included to help elucidate system operations. Do not provide a single comprehensive description and leave it to the reviewer to determine how the system supports specific functionality. Break down how the system supports each function.

Describe how each function, if implemented by the system, is carried out in terms of:

- Inputs
  - Sources of PII, including any that has been created as a result of processing and will be further processed
  - Data sharing agreements with any sources that are non-Exchange entities, including outsourcing and offshoring arrangements
  - How PII is protected in transit if crossing the system boundary and which system component(s) receive it
- Processing
  - What is done with the PII (including creation of new PII) and by which system component(s)
- Outputs
  - The destination of any PII, including any that has been created as a result of processing
  - Data sharing agreements with any destinations that are non-Exchange entities, including outsourcing and offshoring arrangements
  - How PII is protected in transit if crossing the system boundary and which system component(s) it is transmitted from

Indicate whether the system, in support of any of its functions, outsources or offshores PII.

Privacy risk factors include, but are not limited to:

- Incomplete data handling paths
- Data handling paths insufficiently related to a relevant purpose

3.3.1 Consumer Assistance

This function concerns system operations that support consumer assistance, including online, via phone, in-person, and via mail.

[Click **here** and type text here]

3.3.2 Quality Assessment, Disclosures, and Data Reporting

This function concerns evaluation of quality improvement strategies, implementation of enrollee satisfaction surveys, assessment and ratings of healthcare quality and outcomes, and information disclosures and data reporting to CMS.

[Click **here** and type text here]

3.4 Communication Channels

[DI-1(1), IP-1, IP-2, IP-3, IP-4, TR-1]

For each supported communication channel through which the NEE interacts with individuals outside the NEE Partner's organization, describe how notice, consent, access, correction, and complaints are handled and where these processes are documented.

It is expected that each supported communication channel will address each of these elements.

Privacy risk factors include, but are not limited to:

- Limited or no support for some channels
- A channel relying on a different channel for one or more elements (For example, a paper form that only provides a URL for a privacy notice rather than an actual privacy statement is problematic since it assumes that the individual can readily access the URL, even though they are opting to use a paper form. Such arrangements require the NEE to explain why they do not potentially disadvantage individuals.)

Question	Guidance for Responses
Does the website have a posted privacy notice? How is notice provided to individuals?	The response should indicate what informational elements are contained in the notice, such as: • What PII is collected • How the PII is used and disclosed • How long the PII is retained • Access and correction procedures

Question	Guidance for Responses
How is individuals' consent obtained and/or rescinded?	This response should address consent for PII collection, use, and disclosure. In particular, it should address whether there is indication of which requested PII is mandatory and which is voluntary. An example of privacy risk is voluntary collection, use, or disclosure not designated as such.
How can individuals access their PII?	If access procedures are not included in the privacy notice, this response should indicate where individuals can find them. Also indicate any time limits within which the NEE must respond to access requests. Examples of privacy risk are access procedures that are difficult to find and the absence of performance requirements associated with NEE responses.
How do individuals correct their PII?	If correction procedures are not included in the privacy notice, this response should indicate where individuals can find them. Indicate any time limits within which the NEE must respond to correction requests. Explain how downstream entities are notified of corrected or disputed PII. Examples of privacy risk are correction procedures that are difficult to find and the absence of performance requirements associated with NEE responses.
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	If complaint procedures are not included in the privacy notice, this response should indicate where individuals can find them. Also indicate any time limits within which the NEE must respond to complaints. Examples of privacy risk are complaint procedures that are difficult to find and the absence of performance requirements associated with NEE responses.

3.4.1 Online (i.e., Web)

NEE Interaction	How Handled
How is notice provided to individuals?	
How is an individuals' consent obtained and/or rescinded?	
How can individuals access their PII?	
How do individuals correct their PII?	
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	

3.4.2 Phone (i.e., Voice)

NEE Interaction	How Handled
How is notice provided to individuals?	
How is an individuals' consent obtained and/or rescinded?	
How can individuals access their PII?	
How do individuals correct their PII?	
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	

3.4.3 Paper

NEE Interaction	How Handled
How is notice provided to individuals?	
How is an individuals' consent obtained and/or rescinded?	
How can individuals access their PII?	
How do individuals correct their PII?	
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	

3.4.4 In Person (i.e., Assister and/or Office)

NEE Interaction	How Handled
How is notice provided to individuals?	
How is an individuals' consent obtained and/or rescinded?	
How can individuals access their PII?	
How do individuals correct their PII?	

NEE Interaction	How Handled
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	

3.4.5 Other (Specify, e.g., Mobile App)

NEE Interaction	How Handled
How is notice provided to individuals?	
How is an individuals' consent obtained and/or rescinded?	
How can individuals access their PII?	
How do individuals correct their PII?	
How do individuals submit complaints regarding the handling of their PII? How are those complaints adjudicated?	

3.5 Use of Web Measurement and Customization Technologies

Does the site use web measurement and customization technologies (e.g., session cookies)? If so, what type of measurement and customization technologies are used? Are they used to collect PII?

Privacy risk factors include, but are not limited to:

- Accessibility of PII to third-party analytics
- Potential quasi-identifiers in collected data

[Click **here** and type text here]

3.6 Continuous Monitoring

[AR-4]

For the following questions, describe the ways in which the system is monitored to ensure compliance with privacy policies and procedures. Continuous monitoring includes both periodic monitoring and constant monitoring. For example, data loss prevention (DLP) technology can constantly monitor outbound network traffic to detect unencrypted PII. This contrasts with, for example, periodic configuration checks of system components.

3.6.1 Privacy Control Assessment

Describe how privacy controls are assessed on an ongoing basis to ensure they are operating properly and effectively.

This question applies to administrative and operational as well as technical controls and addresses internal rather than external assessments. The response to this question should cover both periodic and constant assessment processes. For example, periodic incident response exercises constitute privacy control assessments. In responding to this question, it may be helpful to review the privacy controls in the SSP and identify what internal assessments are performed. However, it is not necessary to describe how each individual control is assessed. It is sufficient to describe general processes and where they are documented and to note any controls that do not have assessment processes.

Privacy risk factors include, but are not limited to:

- Insufficient periodic assessment frequency or coverage (i.e., the size of the partial set of controls being assessed)
- Insufficient review or analysis of results from constant assessment processes
- Excessive lag time in deriving actionable information from results of constant assessment processes

[Click **here** and type text here]

3.6.2 Auditing

In the table below describe how system auditing take place, including what logs are maintained, summaries of what information is captured in those logs, and how and how often logs are reviewed or analyzed for anomalies.

This question applies to manual as well as automated logs. The response should, where applicable, reference system components described in the response to subsection 3.3. It should also include any auditing of disclosure records (see subsection 3.6.3). Any specific tools used to maintain and analyze logs should be briefly described.

Privacy risk factors include, but are not limited to:

- Inadequate information available to make determinations regarding the appropriateness of PII handling across system operations
- Invalidated metrics
- Insufficiently frequent review and analysis to enable timely responses
- Insufficiently minimized PII in logs

Log	Information Captured	Review/Analysis Method and Frequency

3.6.3 Accounting of Disclosures

[AR-8]

Explain how the system maintains a record of PII disclosures made outside of routine business processes, including by request of the individual to whom the PII pertains. If records consist of automated logs, explain how a specific record or set of records will be retrieved if required.

Note: Such disclosures do not include disclosures to an individual of their own PII.

Typically, the existence of a data sharing agreement with another organization signifies that covered PII disclosures are routine business processes supporting specific system functionality. Therefore, this question addresses instances in which PII is disclosed to another organization (or specific persons) in the absence of such an agreement, i.e., as an exception rather than a routine event.

Such disclosures may be captured and documented manually or via automated mechanisms. If the former, indicate where this process is documented. If the latter, explain how the mechanism captures the necessary information and how, if necessary, information regarding a specific disclosure would be located and produced. This response should confirm that the NEE retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and makes the accounting of disclosures available to the person named in the record upon request.

Privacy risk factors include, but are not limited to:

- Insufficiently documented manual process
- Excessively complex recording or retrieval process
- Insufficiently granular collection of disclosure details, including reason
- Insufficiently minimized PII in disclosure records

[Click **here** and type text here]

3.7 Assessment of Risks

Complete the table below to describe the risk factors identified in Sections 3. This will assist in determining risks and gauging their potential impact on the organization and individuals.

Noncompliance with a required control is by definition a risk factor and should be noted in the table below. Compensating controls are acceptable when circumstances prevent directly mitigating the risk factor or as a temporary measure while directly applicable controls are in the process of being implemented. Compensating controls must be clearly explained and justified. Decisions can then be made regarding requirements to mitigate the risks of collecting, using, maintaining, and disseminating PII. Delete the examples from the final version of this document.

Applicable Risk Factor	Potential Impact of Risk Factor	Compensating Controls and Justification	Additional Planned Controls
Example: Audit logs containing PII are not being reviewed.	Potential exposure of individual PII to unauthorized individuals	Least Privilege procedures in place	Role based access controls in place. These roles include system administrators with privileged access. These roles are reviewed on a quarterly basis
Example: No access control procedures in place for individuals to amend or correct their PII.	Individuals unable to review and/or obtain access to their PII. Reduction in public confidence	Process in place for accounting of disclosures	The access control procedures are currently in draft and will be finalized within the next 30 days.

4. PII Assessment

This section addresses the specific treatment of Personally Identifiable Information (PII) by the NEE.

PII includes, but is not limited to:

- Name
- Date of Birth (DoB)
- Social Security Number (SSN)
- Taxpayer Identification Number (TIN)
- Employment status
- Income
- Citizenship
- Immigration documents
- E-mail
- Phone number
- Address
- Insurance member identification/policy number
- Military status
- Race
- Photographic, audio, and/or video identifiers
- Driver's license number
- Mother's maiden name
- Financial account info
- Legal documents
- Device identifiers

4.1 PII Uses

[AP-1, AP-2, UL-2]

Complete the following table for each function listed in subsections 3.3.1 and 3.3.2. Explain what PII from the relevant population is created and used, and for what purpose.

Privacy risk factors include, but are not limited to:

- Insufficient alignment between population, PII types, and purpose

Population	Consumer Assistance	QA & Reporting
Applicants	PII Types: Purpose:	PII Types: Purpose:
Enrollees	PII Types: Purpose:	PII Types: Purpose:
Beneficiaries / Recipients	PII Types: Purpose:	PII Types: Purpose:

Population	Consumer Assistance	QA & Reporting
Business Partners / Contractors	PII Types: Purpose:	PII Types: Purpose:
Application Counselors	PII Types: Purpose:	PII Types: Purpose:
NEE Personnel	PII Types: Purpose:	PII Types: Purpose:
Other (Specify)	PII Types: Purpose:	PII Types: Purpose:

4.2 Data Quality and Integrity

[DI-1]

The following entries address how the NEE ensures the quality and integrity of PII through automated mechanisms and documented processes.

The responses should explain, in detail, how the NEE checks for and corrects any inaccurate or outdated PII used by its programs/systems and issues guidance ensuring and maximizing the quality of the information collected. Furthermore, the responses should indicate where these processes are documented.

4.2.1 Accuracy

[DI-1(1)]

Describe the processes used to reduce the risk of errors of the PII in the system.

The response should describe how the NEE will confirm the information entered in the system is accurate (e.g., validation against other sources), including information received from third parties. Explain whether the NEE performs periodic quality checks, manually verifies data, implements error-correcting forms, or carries out automated consistency checks.

Privacy risk factors include, but are not limited to:

- Insufficiently or excessively restrictive PII input mechanisms (For example, use of text fields for capturing date of birth rather than pick lists.)
- Insufficient ability to correct pre-populated PII in situ
- Insufficient opportunities to verify PII

[Click **here** and type text here]

4.2.2 Completeness

Explain how the data is checked for completeness.

Describe how the NEE determines what PII is necessary for a given use and ensures that it is available prior to processing and/or decision making.

Privacy risk factors include, but are not limited to:

- Default or null values used in place of necessary data
- Completeness checks performed downstream rather than upstream
- Insufficient opportunities to verify PII

[Click **here** and type text here]

4.2.3 Data Currency

Explain the measures that are taken to ensure the data is current.

Describe any NEE system processes which are designed to ensure that outdated PII is updated or removed from the system. Describe how the NEE revalidates the PII held to maintain currency.

Privacy risk factors include, but are not limited to:

- Insufficiently frequent updates from third-party PII sources
- Limited or delayed propagation of updates across relevant organizational systems

[Click **here** and type text here]

4.3 Minimization of PII

[DM-1, DM-1(1)]

The entries in this subsection focus on methods in place to reduce privacy and security risk through the minimization of PII elements collected, used, disclosed, and/or retained. These methods and processes include the use of access controls, managing the PII inventory, establishing data retention schedules and the use of anonymization and de-identification techniques.

4.3.1 PII Inventory

[SE-1]

Describe the PII inventory process and how it is employed to keep track of the types of PII within the system, including where this process is documented, and how the resulting inventory is used to ensure the PII is relevant and consistent with notices.

Maintaining the PII inventory can be a manual, automated, or semi-automated process. The inventory should reflect the PII data elements currently being maintained.

Privacy risk factors include, but are not limited to:

- Insufficient integration of inventory processes into development and acquisition processes
- Excessive reliance on manual processes for managing the inventory
- Excessive time lag between operational and inventory changes

[Click **here** and type text here]

4.3.2 Access Controls

[UL-1]

These entries focus on how logical, administrative and physical access controls are implemented to safeguard PII.

These responses should provide a high-level overview of the systems technical, administrative, and physical controls used to secure PII. Access to information should be based on a need to know basis.

4.3.2.1 Logical

Explain what are the unique user identification and authentication methods used to access data in the system. The response should describe the automated identity and access management mechanisms used to control electronic access to the system and its data.

Privacy risk factors include, but are not limited to:

- Insufficiently disjoint roles and privileges (i.e., there are large overlaps in privileges across different roles)

[Click **here** and type text here]

4.3.2.2 Administrative

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

Access to PII should be restricted to those with a need-to-know and based on user roles and responsibilities. Explain the criteria, procedures, and responsibilities for granting access (e.g., does access require manager approval) and where this information is documented. For example, will users have access to all data or will access be restricted? Is the assignment of roles documented and maintained?

Privacy risk factors include, but are not limited to:

- Large numbers of roles are common across personnel

[Click **here** and type text here]

4.3.2.3 Physical

Describe the physical safeguards currently in place to protect access to PII from unauthorized intrusions and environmental and natural hazards.

Privacy risk factors include, but are not limited to:

- Insufficient verification and monitoring of external technology support personnel who could have access to PII

[Click **here** and type text here]

4.3.3 Data Retention and Disposal

[DM-2, DM-2(1)]

The following entries in this subsection focuses on the retention and disposal of PII in the system.

4.3.3.1 Schedule

Describe the records retention and destruction schedule for records containing PII, including any paper-based records, and where this schedule is documented.

Specify the applicable schedule and where it is documented; do not refer to a collection of schedules and leave it to the reviewer to determine which one applies.

Privacy risk factors include, but are not limited to:

- Insufficiently justified PII retention beyond legal requirements, including in business associate agreements (BAAs) and data use agreements
- Insufficiently granular retention schedules for different types of PII

[Click **here** and type text here]

4.3.3.2 Implementation

Describe the process for disposing of records (e.g., shredding, erasing) containing PII at the end of the retention period, including whether it is automated in any way and where the process is documented.

Note: NIST SP 800-88 provides guidance on media sanitization. Organizations must use legally compliant methods to ensure secure deletion or destruction of PII.

Privacy risk factors include, but are not limited to:

- Excessively manual disposal processes that may allow retention beyond applicable limits
- Multiple copies of PII held across systems, including back-ups

[Click **here** and type text here]

4.3.3.3 Data Transformation

Describe any measures to permit use of retained PII while reducing its sensitivity and risk of disclosure, including any de-identification techniques, and where they are documented.

Note: NIST SP 800-188 provides guidance on de-identifying PII. The steps and methods used to de-identify, redact, or otherwise reduce the sensitivity of PII may vary depending on the circumstances, but should be appropriate to protect the confidentiality of an individual's PII.

Privacy risk factors include, but are not limited to:

- Insufficient analytical validation of the applied transformations (i.e., that the transformations have reduced risk to the extent expected)
- Insufficient operational validation of the applied transformations (e.g., red teaming)

[Click **here** and type text here]

4.4 Ancillary Uses of PII

[DM-3, DM-3(1)]

The entries in this subsection focuses on any ancillary uses of PII for testing, training, or research purposes. There are two distinct aspects to these questions: governance and method.

Note: As DM-3 (Minimization of PII Used in Testing, Training, and Research) states, to the greatest extent possible, PII should not be used when testing or developing an information system. Further, DM-3 (1) (Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques) states the organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Responses should describe both the governing decisions (including criteria) to use PII for testing purposes, and the procedures for doing so (and where they are documented). Do the latter procedures provide for controls comparable to those implemented in the production environment? If not, what compensating controls are applied?

Privacy risk factors include, but are not limited to:

- Insufficient compensating controls to address gaps between production and other environments
- Synthetic PII derived from real PII
- Insufficient controls governing third parties
- Insufficient analytical validation of any applied transformations (i.e., that the transformations have reduced risk to the extent expected)

Insufficient operational validation of any applied transformations (e.g., red teaming)

4.4.1 Testing

Describe how PII is used for testing purposes, including the reason for its use.

Describe the measures used to minimize the risk involved and where this information is documented. If PII is not allowed to be used for testing, please state so.

[Click **here** and type text here]

4.4.2 Training

Describe how PII is used for training purposes, including the reason for its use.

Describe the measures used to minimize the risk involved and where these are documented. If PII is not allowed to be used for training, please state so.

[Click **here** and type text here]

4.4.3 Research

If PII is used for research purposes, describe those purposes and the minimization techniques, including de-identification, and other measures used to protect the PII and reduce the risk of disclosure and where these measures are documented.

[Click **here** and type text here]

4.5 Assessment of Risk

Complete the table below to describe the risk factors identified in Sections 4. This will assist in determining risks and gauging their potential impact on the organization and individuals. Noncompliance with a required control is by definition a risk factor and should be noted in the table below. Compensating controls are acceptable when circumstances prevent directly mitigating the risk factor or as a temporary measure while directly applicable controls are in the process of being implemented. Compensating controls must be clearly explained and justified. Decisions can then be made regarding requirements to mitigate the risks of collecting, using, maintaining, and disseminating PII. Delete the examples from the final version of this document.

Applicable Risk Factor	Potential Impact of Risk Factor	Compensating Controls and Justification	Additional Planned Controls
Example: PII is used for research purposes.	Potential exposure of PII	All users with access to research are identified and authenticated (IA controls in place).	Product has been purchased to monitor access to datasets containing PII used for research purposes. Final implementation scheduled for third quarter.