Sensitive and Confidential Information – For Official Use Only

Centers for Medicare & Medicaid Services

Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems

Version 1.0

July 6, 2020

Table of Contents

1. Introduction

A change is defined as the addition, modification, or removal of anything that could have a direct or indirect effect on services. As part of the continuing efforts to protect the confidentiality, integrity, and availability (CIA) of the information collected, used, disclosed, and/or retained by the Enhanced Direct Enrollment (EDE) Entity's information technology (IT) systems, EDE entities must implement a configuration change control process as described in the Configuration Management (CM) control family and the EDE System Security and Privacy Plan (SSP). Any system changes that include new, enhanced, or updated hardware and software capabilities; or that apply patches for correcting software flows and new security threats; or that execute changes to business functions and data collection, may cause changes to system configurations as well as the security and privacy posture of the EDE Entity's information systems. Consequently, EDE entities must establish internal procedures that require staff to document system changes and evaluate the scope and nature of those changes in terms of their potential security and privacy impact as an essential aspect of the Entity's own change management and continuous monitoring activities.

All changes must be tested, validated, and documented before implementation into the EDE operational environment. If an EDE Entity makes changes to its EDE environment, the EDE Entity must notify the Centers for Medicare & Medicaid Services (CMS) of these changes.

1.1 Purpose

The purpose of the change control process is to maximize the number of successful information technology changes by ensuring that risks have been properly measured; authorizing the changes to proceed; and managing the change schedule. This document establishes the change notification procedures that an approved EDE Entity must follow when making changes to its IT system environment that has been reviewed and/or approved by CMS. The guidance in this document applies to any EDE Entity responsible for managing and administering the security and privacy of their organization's IT systems.

1.2 Configuration Management and Change Control – Background

The EDE SSP security control CM-3, *Configuration Change Control,* under the CM control family, requires that the organization determine the types of changes to the information system that are configuration controlled. Configuration management requires the change control to include a systematic proposal, justification, implementation, test / evaluation, review, and disposition of changes to the system.

The EDE Entity's change control process should include the following activities:

- Reviewing the change and any impacts with all stakeholders
- Testing all changes internally in a dedicated test environment
- Coordinating required testing with CMS (changes with significant security and privacy impact will require auditor testing)
- Modifying all required documentation

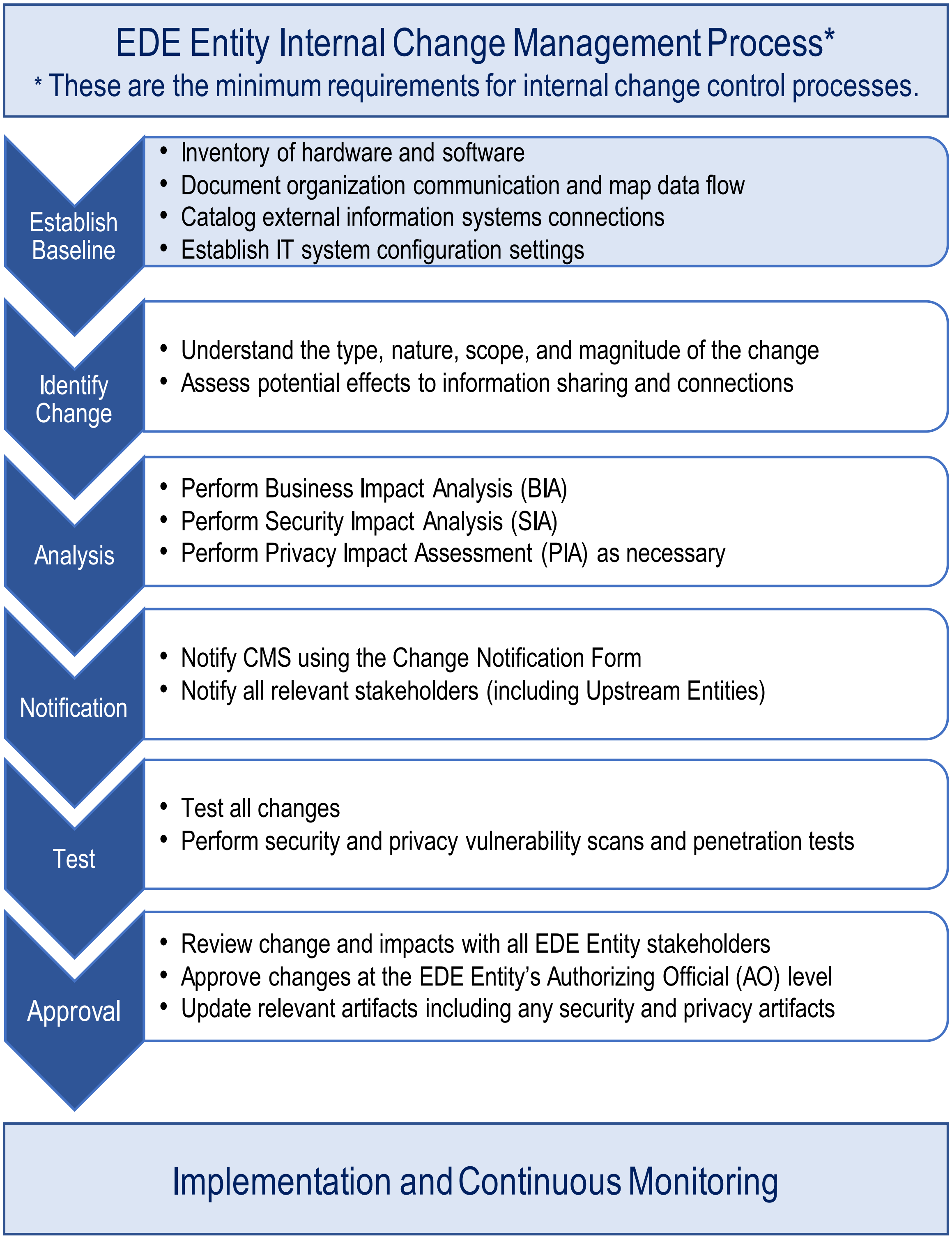
- Updating legal agreements as required
- Approving the changes at the EDE Entity's Authorizing Official (AO) level
- Coordinating production implementation

Any changes to the IT system hardware, software, or firmware components may significantly impact the overall security and privacy posture of a system. To protect the EDE Entity IT systems and the information processed by those systems, the EDE Entity's implementation of configuration management must include a formal change control process as required in the EDE SSP, CM-3: Configuration Change Control. The change control process must contain an evaluation of the security and privacy controls that may be affected by the change and any corresponding information system modifications in support of the change.

2. EDE Entity IT Systems Configuration Management and Change Control Procedures

The change control process is part of a system development life-cycle methodology. Each EDE Entity should ensure that its organization's information security and privacy is planned, managed, and documented throughout the life cycle of the system. **Error! Reference source not found.** depicts the high-level change management and reporting process for EDE Entities.

Figure 1: High-Level EDE Entity IT Systems Configuration Management and Change Control Process



EDE Entity Internal Change Management Process*

* These are the minimum requirements for internal change control processes.

Establish Baseline

- Inventory of hardware and software
- Document organization communication and map data flow
- Catalog external information systems connections
- Establish IT system configuration settings

Identify Change

- Understand the type, nature, scope, and magnitude of the change
- Assess potential effects to information sharing and connections

Analysis

- Perform Business Impact Analysis (BIA)
- Perform Security Impact Analysis (SIA)
- Perform Privacy Impact Assessment (PIA) as necessary

Notification

- Notify CMS using the Change Notification Form
- Notify all relevant stakeholders (including Upstream Entities)

Test

- Test all changes
- Perform security and privacy vulnerability scans and penetration tests

Approval

- Review change and impacts with all EDE Entity stakeholders
- Approve changes at the EDE Entity's Authorizing Official (AO) level
- Update relevant artifacts including any security and privacy artifacts

Implementation and Continuous Monitoring

The EDE Entity must follow these Change Reporting Procedures for its IT systems, including completing the *Change Notification Form for Enhanced Direct Enrollment Entities Information Technology Systems*. Changes related to information sharing and external system connections will likely affect executed legal agreements, including the business agreement. Moreover, the Interconnection Security Agreement (ISA) may require updates to the corresponding agreements, documentation, and artifacts.

2.1 Establish Baseline

Before establishing a change management process, it is essential to have an accurate inventory of hardware and software components with documented configuration baselines. Without an accurate inventory of these components and the configuration baseline, it would be difficult to track changes. The EDE Entity must also maintain a mapping of the information data flow that identifies key stakeholders in the organization who are essential to the operational process and the communication workflow. The EDE Entity must catalog its external information systems connections.

The system configuration baseline establishes the technical components to support the system and includes the business processes supported by the system, the system interconnections, and all information sharing. These baselines and configuration settings are managed and must be documented in the SSP.

This baseline also includes business requirements represented in the CMS-approved audit (e.g., in the CMS-approved business audit toolkits, business report template, and complete mini audit).

2.2 Identify Change

Because IT systems are dynamic, CMS anticipates that all IT systems are in a constant state of change. Therefore, it is critical to understand the type, nature, scope, magnitude, and rationale of the change. Furthermore, the EDE Entity must assess the potential effect of the change to information sharing and internal/external connections.

The EDE Entity must follow the process defined in this subsection. This process is specific to EDE Entity-initiated changes. In Table 1, CMS provides a categorization of the types of changes EDE Entities might make to their EDE environments with examples. These specific changes must be reported to CMS.

2.2.1 EDE Entity-Initiated Change Categories

EDE Entity-initiated changes may include any modifications to the IT systems to the extent that neither the CMS-approved audits nor the existing ISA are accurately reflected. EDE Entities are required to notify CMS of any changes made to their approved EDE environment that fall within the following examples (this is not an exhaustive list of examples – please also refer to Table 1 below):

- Significant changes to the IT system[1]
- Major internal changes to the entity system (such as a major software conversion) that necessitate updating the System Security and Privacy Plan
- Adding new systems to the existing IT systems
- Altering the infrastructure (e.g., moving it from an internal system to an external system)
- Changes to the EDE Entity-to-CMS connection or the EDE Entity-to upstream / downstream entity connection, which include changes in the infrastructure service provider, physical location, or communications protocol changes as specified within the ISA

Table 1 further describes the EDE Entity-initiated change categories. The table serves as a guideline for EDE Entities; EDE Entities must correctly identify the category of each change request (CR) per the CMS-determined definitions of each category. If EDE Entities are unsure which category a change falls in, they should contact the DE Help Desk. CMS will reclassify the category of the CR if the EDE Entity incorrectly identified the category. Certain types of changes are excluded from Table 1; EDE Entities are permitted to fix typos and change design elements (color, font, navigation menus), as long as they are 508-compliant, without notifying CMS. The examples in the third column of Table 1, *Examples of Changes in the Category*, are not exhaustive of all possible category 1, 2, and 3 changes. These examples are provided as guidance to help EDE Entities correctly identify the category of each CR.

[1] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

Table 1. Types of Changes EDE Entities Might Make to Their EDE Environments

Change Category	Brief Description	Examples of Changes in the Category
Category 1: **Changes that require CMS notification with accompanying documentation, but that CMS does not need to approve prior to implementation**	• These changes include any system or software updates that do not alter the privacy and security status of the EDE environment as represented in the CMS-approved audit or changes to the EDE environment that have no effect on the consumer's User Interface (UI) experience. • Can include significant changes in an Entity's communication strategy with consumers that do not impact the UI. • These changes may also include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if CMS has previously messaged that it is a permissible change.	• Changes to application UI text that are not correcting typos • Changes to EDE Entity branding or EDE Entity support channel contact information • Addition of CMS-approved help text language provided in the Application UI Toolkit, Phase 1 Screening Questions, and Phase 2 Screening Questions tabs under the column entitled "Question Help" and the UI Questions tab under the column entitled "Informational Text" • Significant changes in how the Entity communicates with consumers on required actions and about new status information (i.e., communications about notices, data matching issue [DMI] deadlines, etc.) where a significant change in either messaging (that CMS has messaged is permissible), frequency, or method occurs. For example, changing email communications on DMI deadline reminders from once a week to daily or stopping communications (emails, texts, calls) on something the consumer still needs to do.

Change Category	Brief Description	Examples of Changes in the Category
Category 2: Changes that require CMS notification and pre-approval, with accompanying documentation	• These changes include any modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, enrollment processes, status, action items, and related communications about eligibility and enrollment. • These changes do not include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if CMS has previously messaged that it is a permissible change (this falls within Change Category #1, as set forth).	• Minor changes to the consumer's UI, including the application or enrollment experience, that go beyond the changes described in Category #1. For example, changes to the wording of a set of questions and answers not explicitly described in the UI Question Companion Guide or changes to whether previously entered information is pre-populated when the applicant reports a life change. • Changes to the eligibility application that add or remove questions from displaying for any eligibility scenario. An example would be adding a question or tool to help consumers calculate their projected annual income. • Changes to the eligibility application that change the order of questions or the conditional logic for when questions appear. For example, such a change would ask the Medicaid block questions after the income questions instead of before. • Changes to account management capabilities (application and enrollment statuses, notices, consumer action items, etc.). For example, this would entail changing the wording of a set of questions and answers or changes to how DMI and special enrollment period verification issue (SVI) status and notices are displayed and communicated to consumers. • Service area expansion that does not meet the criteria described in Category 3 below.

Change Category	Brief Description	Examples of Changes in the Category
Category 3: Changes that require CMS notification, pre-approval, and verification by an independent third-party Auditor	• These changes include any modifications to the systems comprising the EDE environment to the extent that the CMS-approved audits and the existing Interconnection Security Agreement (ISA) no longer accurately reflect the compliance of the environment.	• Adding new systems to the EDE environment • Significant changes[2] • Moving to a new data center • Altering the infrastructure (e.g., moving it from an internal system to an external system) • Service area expansion that enables an EDE Entity to complete 5 or more Eligibility Results Toolkit test cases it was not previously able to complete but can now complete with the expanded list of states or EDE Entities adding states that differ from its approved use of the EDE pathway in two or more of the following: – Medicaid expansion – Non-Medicaid expansion – CHIP waiting period, and – states with a deprivation requirement

2.3 Analysis

The EDE Entity must perform a Security Impact Analysis (SIA), a Business Impact Analysis (BIA), and potentially an update to their Privacy Impact Assessment (PIA) based on the analysis of the SIA to determine the impact that changes will have on the Entity's IT systems.

The EDE Entity must submit an SIA. According to NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, an SIA is described as:

> … the analysis conducted by qualified staff within an organization to determine the extent to which changes to the information system affect the security posture of the system. Because information systems are typically in a constant state of change, it is important to understand the impact of changes on the functionality of existing security controls and in the context of organizational risk tolerance. Security impact analysis is incorporated into the documented configuration change control process.
>
> The analysis of the security impact of a change occurs when changes are analyzed and evaluated for adverse impact on security, preferably before they are approved and

[2] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

implemented, but also in the case of emergency/unscheduled changes.[3] Once the changes are implemented and tested, a security impact analysis (and/or assessment) is performed to ensure that the changes have been implemented as approved, and to determine if there are any unanticipated effects of the change on existing security controls.

A comprehensive SIA will analyze the impact of the change on both the technical security features that provide essential security functionality and the core business processes that rely on them. The EDE Entity must determine the driver for the change and the nature of the change on the impacted components. The affected components and/or business processes must be cross-referenced to the affected EDE Entity SSP control families during the analysis. The EDE Entity must document the impact of any change to any SSP control family. Potential changes include, but are not limited to:

- Supporting software changes or version upgrades
- Adding services that modify the infrastructure
- Modifying the connection to the CMS Data Services Hub
- Responding to changes in the business process flow
- Changes to how Personally Identifiable Information (PII) is created, collected, disclosed, accessed, maintained, stored, and used
- Adding or modifying applications supporting EDE functions that may impact security and privacy
- Adopting changes in Commercial Off-the-Shelf (COTS) software
- Adapting to hardware or infrastructure changes, such as deployment of cloud technology
- Changing operations at the processing site or outsourcing of data center operations

2.3.1 SIA Checklist

An SIA includes an assessment of the risk associated with the potential change. Based on additional risks introduced with the change, compensating security and privacy controls may be required.

To assist in completing the analysis, CMS has provided the following series of questions to determine possible impacts that the change may have on security controls within each control family. Suggested questions include:

1. **Access Control (AC):** Will change(s) to the system affect how the system limits: (a) information system access to authorized users, (b) processes acting on behalf of authorized users or devices (including other information systems), and (c) the types of transactions and functions that authorized users are permitted to exercise?

[3] In the context of EDE, Entities may only deviate from the notification and approval protocols in the case of emergency. Emergency circumstances may include severe vulnerability patches to hardware or software and newly discovered high-impact vulnerabilities that have already been exploited. This list of examples is not exhaustive of all potential emergencies. Similarly, if EDE Entities identify compliance issues, they should contact the DE Help Desk immediately.

2. **Awareness and Training (AT):** Will change(s) affect required system training to ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities?
3. **Audit and Accountability (AU):** Will change(s) affect (a) how system audit requirements to create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (b) ensure that the actions of individual information system users can be uniquely traced to those users to hold them accountable for their actions?
4. **Configuration Management (CM):** Will change(s) to the system impact the (a) baseline configuration and inventory of organizational information systems; (b) establishment and enforcement of security configuration settings; and (c) ability to monitor and control changes to the baseline configurations and to the constituent components of the systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycle?
5. **Contingency Plan (CP):** Will change(s) to the system impact the (a) contingency plans for emergency response, backup operations, and disaster recovery for organizational information systems, and (b) availability of critical information resources and continuity of operations in emergency situations?
6. **Identification and Authentication (IA):** Will change(s) to the system impact how it (a) identifies users, processes acting on behalf of users, or devices; and (b) authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems?
7. **Incident Response (IR):** Will change(s) to the system impact the (a) operational incident handling capability for the information system, including detection, analysis, containment, recovery, and user response activities; and (b) the ability to effectively track, document, and report incidents to CMS or other external entities?
8. **Maintenance (MA):** Will change(s) to the system impact how (a) periodic and timely maintenance is performed, and (b) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance?
9. **Physical and Environment Protection (PE):** Will change(s) to the system/system environment change how (a) physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals; (b) affect how the physical plant and support infrastructure for information systems are protected; (c) affect how supporting utilities for information systems are provided; and (d) affect how appropriate environmental controls in facilities are provided?
10. **Planning (PL):** Will change(s) to the system/system environment impact the (a) system security plan for information system that describe the security controls in place for the information system and (b) change the rules of behavior for individuals accessing the information systems?
11. **Risk Assessment (RA):** Will change(s) to the system impact (a) how information systems are assessed every three years or whenever a significant change occurs to the

information system to determine if security controls are effective in their application; (b) plans of action with milestones (POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities; (c) authorization for processing including any associated information system connections by a designated senior agency official; and (d) monitoring for continued effectiveness of the controls?

12. **System and Service Acquisition (SA):** Will change(s) to the system affect the information system for (a) any changes to Service Acquisition policy or procedure, (b) how the resources are allocated, (c) any information system documentation, (d) any software usage or implementation, (e) any external services outside of the information boundary, and (f) any internal development or integration?

13. **System and Communications Protection (SC):** Will change(s) to the system affect how (a) communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and key internal boundaries of the information systems; and (b) architectural designs, software development techniques, and systems engineering principles that promote effective information security are implemented?

14. **System and Information Integrity (SI):** Will change(s) to the system affect how (a) system flaws are identified, reported, and corrected in a timely manner; (b) malicious code protection is employed; (c) system events are monitored and detected; (d) the correct operation of security functions is verified; and (e) information is checked for accuracy, completeness, validity, and authenticity?

15. **Accountability, Audit, and Risk Management (AR):** Will change(s) to the system affect how (a) the system is being monitored; (b) how privacy risks are determined; and (c) how the privacy controls are assessed to demonstrate that the organization is complying with all applicable privacy protection requirements to minimize the overall privacy risk?

16. **Data Quality and Integrity (DI**): Will the change(s) affect how the organization assures how PII collected and maintained is accurate, relevant, timely, and complete for the purpose for which it is intended to be used, as specified in public notices?

17. **Individual Participation and Redress (IP):** Will change(s) to the system affect how organizations will provide individuals with the capability to access their PII and to have their PII corrected or amended, as appropriate?

18. **Security (SE):** Will the change(s) affect how (a) the organization maintains and updates the inventory of all programs and systems used for collecting, updating, or sharing of PII, and (b) the PII data elements? **Note:** The EDE Entity should ensure the current inventory of PII is consistent with the PII data elements in the Privacy Impact Assessment.

19. **Transparency (TR):** Will the change(s) affect the current privacy notice or how the organization provides public notice of information practices?

20. **Use Limitation (UL):** Will the change(s) affect how the organization uses PII internally and as identified in the Privacy Act and/or in public notices to include applicable contractual agreements?

When an SIA is completed, it may expose potential vulnerabilities that must be mitigated, including the potential for updating the PIA. Additional safeguards and countermeasures may be required to reduce or eliminate the risk.

2.4 Notification

After correctly identifying the category of the EDE Entity-initiated change, the EDE Entity must notify all stakeholders, including upstream entities and CMS. For proposed category 1 changes, entities must notify CMS and provide the required documentation. For proposed category 2 changes, entities must notify CMS and provide the required documentation at least ten (10) business days in advance of the planned implementation. For proposed category 3 changes, entities must notify CMS and provide the required documentation at least ninety (90) days in advance of the planned implementation to allow time for change coordination, testing, and execution of new legal agreements, if necessary. Category 3 audits can be submitted on a rolling basis. Emergency changes that must be implemented as soon as possible, usually to resolve an incident, can be reported to CMS post implementation. Routine changes, such as monthly patching activities, can be implemented without reporting to CMS.

The EDE Entity's notification to CMS must use the *Change Notification Form for EDE Entity Information Technology Systems* and follow the appropriate process described in subsections 2.4.1–2.4.3.

2.4.1 Change Category 1

Category 1 changes require CMS notification with accompanying documentation, but CMS does not need to approve the change. However, CMS may recategorize the category of the change upon review of the submitted documents. The EDE Entity:

- Must email the DE Help Desk and detail the scope of the change by completing the *Change Notification Form for EDE Entity Information Technology Systems*. The email subject line must start with "EDE Entity initiated CR – Category 1 Change."

- Must submit accompanying documentation, including the SIA and a mockup of the UI or a screenshot from within the EDE Entity's testing environment that demonstrates the intended change, if applicable. Based on a review of the documentation, the PIA may need updating, however, the EDE Entity is not required to submit the PIA to CMS unless it is requested. EDE Entities should submit any accompanying documentation through the secure portal.

2.4.2 Change Category 2

Category 2 changes require CMS notification and pre-approval, with accompanying documentation. The EDE Entity:

- Must email the DE Help Desk and detail the scope of the change by completing the *Change Notification Form for EDE Entity Information Technology Systems*. The email subject line must start with "EDE Entity initiated CR – Category 2 Change."

- Must submit accompanying documentation through the secure portal including the SIA and a mockup of the UI or a screenshot from within the EDE Entity's testing environment that demonstrates the intended change, if applicable.

This type of change requires pre-approval from CMS. CMS will review the change and respond to the EDE Entity. CMS cannot guarantee a response timeframe. CMS will either confirm that the EDE Entity can proceed or may request additional information.

2.4.3 Change Category 3

Category 3 changes require CMS notification, pre-approval, and verification by an independent third-party Auditor. The EDE Entity:

- Must email the DE Help Desk for pre-approval before implementing the change and detail the scope of the change by completing the *Change Notification Form for EDE Entity Information Technology Systems*, describing how the Auditor will review the change, and specifying what documentation the Auditor will prepare. The email subject line must start with "EDE Entity initiated CR – Category 3 Change."
- Must submit accompanying documentation through the secure portal including the SIA and a mockup of the UI or a screenshot from within the EDE Entity's testing environment that demonstrates the intended change, if applicable.

  The documents prepared by the Auditor include an updated POA&M, updated toolkits (as applicable), an updated Security and Privacy Assessment Report (SAR), vulnerability scans, and an updated IT systems penetration test. EDE Entities must submit accompanying documentation through the secure portal.
- Will fulfill the following requirements with respect to the Auditor Contract and Audit Kick-Off:
  - Auditor Contract: CMS requests a copy of the signed agreement or contract between the Auditor(s) and primary EDE Entity. The contract must describe the Auditor's entire scope of work. The primary EDE Entity may redact information (e.g., pricing) that is not necessary for CMS review.
  - Security Assessment Plan (SAP): Submission of a Security Assessment Plan (SAP) prior to the start of the assessment is required. Approval from CMS is not required prior to kicking off the audit. However, CMS would like the opportunity to review the plan to ensure all assessment elements are included.
  - Kick-Off Call: if the EDE Entity is working with a new auditor (i.e., not the auditor that completed the prior P&S audit) it must schedule a kickoff call. If the auditor has not changed but the EDE Entity would like to arrange a call for the existing auditor, it does have the option to request a kickoff call, but it would not be required.
- Must submit required documentation through the secure portal after the third-party Auditor verifies the change. CMS will review the change and respond to the EDE Entity. CMS cannot guarantee a response timeframe. CMS will either confirm that the EDE Entity can proceed or may request additional information.
- May be required to re-execute the ISA.

2.5 Test

All changes must be tested, validated, and documented before promotion to the operational environment. The EDE Entity must build a master test plan and strategy that encompasses all impacted components. The testing strategy must include end-to-end, regression, and acceptance testing.

The EDE Entity must have a separate test environment and a pre-production environment that hosts an instance of the production operational environment. These testing and pre-production environments should mirror the production environment to generate an accurate response to changes as they are made for testing. Systems can be tested in a test environment provided these environments mirror the production environment. However, a pre-production environment must reflect production at all times, and therefore must not be used for testing. The EDE Entity should properly document any deviations in the environment used for testing.

The EDE Entity must perform security and privacy vulnerability scans and penetration tests within the pre-production environment. The EDE Entity will certify and attest that all system vulnerabilities found as a result of security and privacy audits performed in a pre-production environment will also be mitigated in the production environment. Depending on the change category, independent third-party Auditor testing may be required.

2.6 Approval

The EDE Entity must review all changes and their impacts with all relevant EDE Entity stakeholders, including Upstream EDE Entities. The EDE Entity's AO, who is responsible for overseeing the security and privacy of the EDE IT system, must review all security and privacy documentation impacted by the change. The EDE Entity's AO should use this information to make a risk-based approval decision. The EDE Entity must update relevant security and privacy artifacts as necessary.

For EDE Entity-initiated change categories 2 and 3, CMS will review the change and will either confirm that the EDE Entity can proceed or may request additional information. CMS cannot guarantee a response timeframe.