DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information & Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201

July 26, 2019

Frequently Asked Questions (FAQs) Regarding Enhanced Direct Enrollment (EDE) Information Security and Privacy Continuous Monitoring (ISCM Strategy)

1. Do all EDE Entities need to adhere to the Information Security and Privacy Continuous Monitoring (ISCM) Strategy?

The ISCM Strategy is for approved EDE Entities.[1] Once a prospective EDE Entity receives CMS Request-To-Connect (RTC) approval and authorization, the approved EDE Entity must adhere to the continuous monitoring requirements in the ISCM Strategy Guide. The ISCM Strategy Guide provides the minimum reporting requirements to CMS in order to maintain ongoing CMS RTC authorization and approval including the completion of an annual assessment of security and privacy core controls.

Prospective EDE Entities should be implementing an internal information security and privacy continuous monitoring program as part of comprehensive cybersecurity best practices.

2. When does the ISCM process for approved EDE Entities kick in?

Once a prospective EDE Entity receives CMS RTC approval and authorization, approved EDE Entities must adhere to the continuous monitoring reporting requirements in the ISCM Strategy Guide which includes the completion of an annual assessment of security and privacy core controls described in the ISCM Strategy Guide.

3. What are the ISCM submission requirements to CMS and timeframe?

The following submission requirements are for approved EDE Entities only:

- **Quarterly – Plan of Action and Milestones (POA&M) submissions by the last business day of:**
  - March
  - June
  - September
  - December

  Note: Unless there are outstanding weaknesses for which CMS would require monthly submissions until all major significant or major findings are resolved.

[1] This includes all primary EDE Entities and any upstream EDE Entities that submitted a supplemental privacy and security audit to document the compliance of any additional systems or functionality. Please refer to the FAQ [*insert title]* and the EDE Guidelines Section IV.B ("Providing an EDE Environment to Other Entities") available at: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf.

- **Annual (by the last business day of September):**
  - Annual Security and Privacy Assessment Report (SAR) of the CMS defined subset of security and privacy core controls
  - Annual Penetration test results during reauthorization
  - Annual System Security and Privacy Plan (SSP) updates
  - Most recent three (3) months of the vulnerability scans
  - POA&M updates

4. **What are the internal EDE Entity ISCM activities?**

In addition to the CMS reporting requirements, the approved EDE Entity must maintain the following internal activities:

- **Monthly:**
  - POA&M updates
  - Vulnerability scans

- **Quarterly:**
  - Continuous monitoring reports should follow the reporting requirements identified in EDE SSP CA-7 Continuous Monitoring control

- **Annual:**
  - Annual System Security and Privacy Plan (SSP) updates

Refer to the ISCM Strategy Guide Table 2, for a comprehensive list of internal EDE Entity activities. An "X" in the "NEE-Authored Deliverable" column indicates an internal EDE Entity activity.

5. What is the scope of the annual security and privacy assessment?

The approved EDE Entity is required to have an Auditor perform an annual assessment of a subset of the overall security and privacy controls implemented on the approved EDE environment documented in the ISCM Strategy Guide Table 3. Furthermore, the CMS ISSO may select additional controls for testing to assess the security and privacy risk posture based on evolving threats, demonstrated weaknesses, and any potential changes to the approved EDE environment. The CMS ISSO has the option to vary the total number of controls tested that is commensurate with the level of risk.