Centers for Medicare & Medicaid Services

Affordable Care Act (ACA) Health Insurance Administering Entity

Annual Security and Privacy Attestation Procedures for the Affordable Care Act Information Systems

Final

Publication Date:[MM DD, YYYY]

Version 2.3

Record of Changes

Version Number	Version Date	Author/ Owner	A=Add, M=Modify, D=Delete	Description of Change	Substantive Change [Y/N]
1.0	10/2014	-	**N/A**	Final draft	**N/A**
2.0	03/2016	-	**A**	Final Draft (Privacy Updates)	**Y**
2.1	03/2018	-	**M**	Final (updated for 2018)	**N**
2.2	03/2019	**Dennis Cooper**	**M**	Final (updated for 2019)	**Y**
2.3	03/2020	**S. Sean Jensen**	**M**	Final (updated for 2020)	**N**

Table of Contents

1. Introduction 3

1.1 Requirements Background 3
1.2 Purpose 3

2. Annual Security and Privacy Attestation 3

2.1 Annual Security and Privacy Self-assessment 3
2.2 Annual Security and Privacy Independent Assessment 4
2.3 Annual Security and Privacy Attestation Process 4
2.4 Attestation Testing 5

3. Annual Security and Privacy Attestation Report 6

4. Submission Timeframe 6

1. Introduction

The Annual Security and Privacy Attestation Procedures for the Affordable Care Act (ACA) Information Systems provides guidance and the report template for the annual attestation of the Minimum Acceptable Risk Standards for Exchanges (MARS-E) security and privacy controls mandated by the Centers for Medicare & Medicaid Services (CMS). The annual attestation is one of the activities associated with the security control continuous monitoring process and the privacy controls including privacy impact, risk assessment, monitoring, and auditing.

1.1 Requirements Background

The basis for the annual security and privacy attestation is the MARS-E Security Assessment Control (CA-2). This control requires that all MARS-E security and privacy controls, attributable to a specific system or application, be assessed over a three-year period with a subset of the controls assessed annually during the annual attestation process. Additionally, the MARS-E Continuous Monitoring Control (CA-7) requires organizations to implement a continuous monitoring program that includes reporting of the security state of the information system to appropriate organizational officials every 365 days. The enforcement of these controls supports the identification of significant security vulnerabilities by recognizing non-compliant control areas in a timely manner. The MARS-E Privacy Impact and Risk Assessment Control (AR-2) is also part of this annual review.

The assessment and resulting attestation report provided to CMS help identify and address systemic security and privacy issues and provides a detailed understanding of the current security and privacy posture associated with the broader ACA program.

1.2 Purpose

This document provides guidance and direction for:

- Ensuring ACA systems comply with MARS-E
- Testing at least one-third of the MARS-E security controls annually
- Testing privacy controls
- Reviewing and updating ACA systems security and privacy documentation
- Completing and submitting the Annual Security and Privacy Attestation Report

2. Annual Security and Privacy Attestation

The annual security and privacy control attestation may be conducted by the Administering Entity (AE) business owner, the system owner, the system developer/maintainer, or by an independent assessor.

2.1 Annual Security and Privacy Self-assessment

If a self-assessment is performed for the annual attestation, the test results must be documented and submitted to CMS utilizing the following:

- Annual Security and Privacy Attestation Report

All weaknesses identified during a self-assessment need to be captured in the Plan of Actions & Milestones (POA&Ms).

2.2 Annual Security and Privacy Independent Assessment

If an independent assessment is performed for the annual attestation, the test results must be documented and submitted to CMS utilizing the following:

- Security and Privacy Assessment Plan (SAP)
- Security and Privacy Assessment Report (SAR)
- Annual Security and Privacy Attestation Report

The SAP and SAR would be applied to the Y1, Y2, and Y3 security and privacy control testing necessary for the renewal of an Authority to Connect (ATC).

All weaknesses identified during an independent assessment need to be captured in the Plan of Actions & Milestones (POA&Ms).

2.3 Annual Security and Privacy Attestation Process

The annual security and privacy attestation process includes the following activities by the AE:

- Review the AE's policies and procedures and attest to their implementation
- Determine security and privacy controls to be tested including:
  - Control families for current year (See Annual Security and Privacy Attestation Template instructions)
  - Controls to be tested annually (See Annual Security and Privacy Attestation Template instructions)
  - Controls with identified weaknesses closed during the current year *(Note: completed/closed findings on the Plan of Action and Milestones (POA&M) should remain on the POA&M 1 year)*
  - Controls impacted by changes to the system environment during the current year
- Review and evaluate ACA security and privacy documentation by the Administering Entity. The assessment and resulting attestation report must be submitted to CMS.
  - Information Security Risk Assessment (ISRA) to determine:
    - Significant changes to business objectives or overall mission importance
    - Significant changes to the security state due to new or modified federal legislation, regulations, directives, policies, standards, or guidance
    - Effectiveness of security controls changed during the past year
    - New vulnerabilities affecting the overall risk to the system found during continuous monitoring activities, the annual security and privacy attestation process, and the independent security assessment process
  - System Security Plan (SSP) including the security and privacy implementations to verify the system information and control implementation documented is correct and updated as necessary
  - Contingency Plan (CP) and the Annual CP Test with the following:

  - Validate the Maximum Tolerable Disruption (MTD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
  - Test and exercise the CP using the CP Test Plan
  - Document the results of the CP test in a report
  - Update the CP based on the test results

- Review the Privacy Impact Assessment (PIA) to verify that privacy controls are documented, privacy risks are assessed, and control implementations have not changed
- Review legal agreements with CMS and other business partners to ensure they are current. These agreements include:
  - Interconnection Security Agreement (ISA)
  - Computer Matching Agreement (CMA)
  - Information Exchange Agreement (IEA)
  - Other forms of agreements such as data use agreements

2.4 Attestation Testing

The AE may fulfill the annual attestation requirement by using the current year's security and privacy control assessment results from any of the following sources, including but not limited to:

- An independent assessment
- Assessments conducted as part of an ATC or reauthorization
- Continuous monitoring activities
- Ongoing testing and evaluation of security and privacy associated with the system development life cycle
- Internal Privacy Risk Assessments
- Audits from the Office of the Inspector General (OIG), the General Accounting Office (GAO), or the Internal Revenue Service (IRS)

Depending on the extent of testing from other sources, the organization may need to perform additional testing to ensure all security controls are reviewed and validated against the MARS-E required controls. For testing the controls, the procedures for each control are documented in MARS-E.

The use of automated support tools (e.g. vulnerability scanners, patch management and configuration management software solutions) facilitates near real-time risk management by tracking violation and compliance changes. These types of tools and the associated reporting performed can assist the AE in validating the adequacy of security and privacy control implementations.

Only control testing performed within three months prior to the June submission timeline will be accepted for the current year's annual attestation.

If leveraging independent assessment results as part of a current year ATC or reauthorization, only testing performed within three months prior or three months post the June submission timeline will be accepted for the current year's annual attestation. Prior approval from your CMS

Information System Security Officer (ISSO) for attestation submissions that will occur after the June 30th due date must be received to ensure accurate compliance tracking.

3. Annual Security and Privacy Attestation Report

The Annual Security and Privacy Attestation Template must be used to complete the annual security and privacy attestation. The signatories on the report personally attest to the report's accuracy and authenticity.

In addition to the information to be completed for the controls, the summary section of the report requires the latest review date for the following security documents:

- Authority to Connect (ATC)
- System Security Plan (SSP) and supporting Attachments
- Security and Privacy Assessment Report (SAR)
- Information Security Risk Assessment (ISRA)
- Contingency Plan (CP)
- Contingency Plan Test Date (CPT)
- Privacy Impact Assessment (PIA)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Plan of Actions & Milestones (POA&Ms)
- Legal Agreements such as the Computer Matching Agreement (CMA)
- Information Exchange Agreement (IEA)
- Organization Continuous Monitoring Policies and Procedures
- Interconnection Security Agreement (ISA)

Please note these documents are not required to submit to CMS as part of the annual attestation submission but should be available should CMS request them.

4. Submission Timeframe

The Annual Security and Privacy Attestation Report is due to CMS no later than June 30th of each year or the first business day after should June 30th fall on a weekend.

Prior approval from your CMS ISSO for attestation submissions that will occur after the June 30th due date (or first business day after) must be received to ensure accurate compliance tracking. Please note that any expected delays of attestation submissions should also be communicated to your CMS ISSO.