Sensitive and Confidential Information – For Official Use Only

Enhanced Direct Enrollment Entity Name (Acronym)

Security and Privacy Assessment Report of the <Name of Enhanced Direct Enrollment Entity>

<Name of EDE Information System>

As performed by <Auditor Company Name>

SAR Version 0.1

Report Publication Date

CMS SAR Template v 2.0

Security and Privacy Assessment Report

Prepared by: <Identify Independent Third-Party Auditor that prepared this document>

Organization Name: <Enter Company/Organization>.
Street Address: <Enter Street Address>
Suite/Room/ Building: <Enter Suite/Room/Building>
City, State Zip: <Enter Zip Code>

Prepared for: <Identify Enhanced Direct Enrollment Entity>

Organization Name: <Enter Company/Organization>.
Street Address: <Enter Street Address>
Suite/Room/ Building: <Enter Suite/Room/Building>
City, State Zip: <Enter Zip Code>

Revision History

Date	Description	Version of SAR	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

Table of Contents

List of Tables

1. Introduction and Purpose

The Patient Protection and Affordable Care Act (ACA) program requires a Non-Exchange Entity (NEE) to use an independent third-party Auditor to perform security and privacy assessment testing and to develop a Security and Privacy Assessment Report (SAR) based on the outcomes of the assessment. Enhanced Direct Enrollment (EDE) Entities are considered NEEs. The < Auditor Name> performed security and privacy testing for <Information System Abbreviation> in accordance with the <Information System Abbreviation> Security and Privacy Controls Assessment Test Plan (SAP), <SAP Date>, <SAP Version #>.

This SAR provides the < EDE Entity> ISSO, SOP, and the AOs with the results of the assessment completed for the <Information System Abbreviation>. The SAR describes risks associated with the vulnerabilities identified during the <Information System Abbreviation> independent security and privacy assessment and serves as the risk summary report as referenced in the Framework for Independent Assessment of Security and Privacy Controls for EDE Entities and NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

1.1 Applicable Laws, Regulations, and Standards

By interconnecting with the CMS network and the CMS information system, the EDE Entity agrees to be bound by the EDE Interconnection Security Agreement (ISA) and the use of the CMS network and information system in compliance with the ISA. The following applicable laws, regulations, and standards apply (the EDE Entity may also add state laws, regulations, and standards as applicable):

- Federal Information Security Management Act of 2014 (FISMA)
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information
- Privacy Act of 1974, 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA) of 1966 (P.L. 104-191)
- Patient Protection and Affordability Care Act of 2010
- HHS Regulation, 45 CFR § 155.260 – Privacy and Security of Personally Identifiable Information
- HHS Regulation, 45 CFR § 155.280 – Oversight and monitoring of privacy and security requirements
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*

1.2 Scope

The Auditor analyzed all assessment results to provide the < EDE Entity> Information System Security Officer (ISSO), Senior Official for Privacy (SOP), and the Authorizing Officials (AO) with an assessment of the security and privacy controls that safeguard the confidentiality, integrity, and availability (CIA) of data hosted by the system as described in the <Information System Abbreviation> System Security and Privacy Plan (SSP).

This document consists of a SAR for <Information System Name> <Information System Abbreviation> as required by <*Insert reason for the assessment*>. This SAR presents the results of a security and privacy test and evaluation of the <Information System Abbreviation> and is provided to support the <Name of EDE Entity> <Acronym of EDE Entity> program goals, efforts, and activities necessary to achieve compliance with the necessary security and privacy requirements.

The <EDE Entity> engaged < Auditor Name > to perform an onsite security and privacy controls assessment (SCA) of the <Information System Name> to determine:

- If the system is in compliance with the CMS security and privacy standards described in the EDE SSP;
- If the underlying infrastructure supporting the system is secure;
- If the system and data are securely maintained; and
- If proper configuration associated with the database and file structure storing the data are in place.

The SCA consisted of system components and documentation reviews. The following components were tested during this assessment:

Instruction: Provide a list of components (e.g., hardware, software, etc.) that were planned to be tested and those that were actually tested during the assessment. These components may be items identified in the SAP, Section 2. Include additional documents as necessary.

- Example: Operating system(s): Windows, Linux and version
- Example: Database and version #
- Example: Information System, and sub components
- Example: Web Applications and URLs

[Delete this and all other instructions examples from your final version of this document.]

Instruction: Security and privacy documentation will be reviewed for completeness and accuracy Through this process, the Auditor will gain insight to determine if all conrrols are implemented as descried. The Auditor's review also augments technical control testing.

The Auditor must review, at a minimum, the following required documents for assessment Additional documents or supporting artifacts may be reviewed as necessary.

[Delete this and all other instructions from your final version of this document.]

The following documents will be assessed:

- Business Agreement with Data Use Agreement (DUA);
- Configuration Management Plan (CMP);
- Contingency Plan (CP) and Test Results;
- Plan of Action and Milestones (POA&M);
- System Security and Privacy Plan (SSP) Final;
- Incident Response Plan (IRP) and Incident/Breach Notification and Test Plan;
- Privacy Impact Assessment (PIA) and other privacy documentation, including, but not limited to, privacy notices as well as agreements to collect, use, and disclose Personally Identifiable Information (PII) and Privacy Act Statements;
- Security Awareness Training (SAT) Plan and Training Records;
- Interconnection Security Agreements (ISA);
- Information Security Risk Assessment (ISRA);
- Governance documents and privacy policy; and
- Documentation describing the organization’s privacy risk assessment process and documentation of privacy risk assessments performed by the organization.

2. System Overview

2.1 System Description

Instruction: In this subsection, insert a general description of the information system. The description should be consistent with the description found in the SSP. The description in this subsection may differ only if additional information is included that is not available in the SSP or if the description in the SSP is not accurate.

[Delete this instruction and all other instructions from your final version of this document.]

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

2.2 Purpose of System

Instruction: Insert the purpose of the information system. The purpose must be consistent with the SSP.

[Delete this instruction and all other instructions from your final version of this document.]

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

3. Executive Summary Report

The Auditor has complied with the terms articulated in the SAP and the assessment is complete and comprehensive. Appendices A through C provides the infrastructure, database, web application scan results. Appendix D provides the penetration test report which includes test results for all components within scope of the information system. Appendix E provides the summary results of all scans.

3.1 Summary of Findings

Instruction: Provide a narrative summary of the findings relating to the security and privacy control families. Complete the summary findings table 1 for ALL findings from the assessment regardless type of test. Refer to subsection 4.1 for a description of the column headings.

The Auditor must provide a total of number system risks that were identified for the information system. The Auditor must identify the number of High risks, Moderate risks, and Low risks for all findings, including but not limited to, scan results, penetration test results, interviews, and control test results. Priority levels are based on the type of vulnerability identified.

For example, many of the findings fall into the Access Control (AC) family due to the misconfiguration of the database and web application services, and overdue account reviews.

[Delete this instruction and all other instructions from your final version of this document.]

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

Table 1. Summary Findings Table

Row #	Weakness	Risk Level	Control #	POA&M Reference #

3.2 Summary of Recommendations

For each finding, the Auditor developed detailed recommendations for improvements that address the findings and the business and system risks. Most of the recommendations in this document fall into the following areas:

Instruction: While all findings must be addressed, findings representing a high business risk should be mitigated or closed immediately to reduce the risk exposure. The following example list of findings areas should be modified based on the SCA results:

- Block Unused Ports and Protocols:
- Perform Security and Privacy Monitoring:
- Strengthen Database Access Controls:
- Update Documentation:

Provide a summary of recommendations grouped by families, if possible. Identify which corrective actions can mitigate large groups of findings.

For example: The Access Control (AC) and most of the Configuration Management (CM) findings can be remediated if the database is upgraded to the latest version of the software, and necessary hot fixes and patches are applied.

[Delete this instruction and all other instructions from your final version of this document.]

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

4. Detailed Findings Report

Instruction: Provide a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Include findings from all scans and tests. For each vulnerability, provide the following:

- Explanation of the vulnerability
- Identification of specific risks to the continued operations of the system
- Analysis of impact of each risk
- Suggested corrective actions for closing or reducing the impact of each vulnerability

[Delete this instruction and all other instructions from your final version of this document.]

4.1 Detailed Findings Table

Instructions: This subsection provides a description of the columns in the Detailed Findings Table (Table 3) in subsection 4.2.

Row Number

Each finding has a row number included to provide easy reference for briefings and cross-referencing.

POA&M Reference

Verify that the findings are identified in the Plan of Action and Milestones (POA&M).

Weakness

The Weakness column provides a brief description of the security and privacy vulnerability.

Risk Level

Each finding is considered a business risk and assigned a risk level rating of high, moderate, or low. The rating provides an assessment of the magnitude of the finding and helps establish a priority for addressing the vulnerability. **Error! Reference source not found.** defines the Risk levels.

Table 2. Definition of Risk Levels

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment.
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment.

Control Number

The Control Number column identifies the EDE security and privacy control family and control number that is affected by the vulnerability, for example, (AC)-1: Access Control.

Center for Internet Security (CIS) Top 20 Control

State whether the control falls under a CIS Top 20 control area.

Open Web Application Security Project (OWASP) Top 10

State whether the finding falls under one of the OWASP Top 10 most critical web application security risks.

Affected Systems

The systems, URLs, IP addresses, etc., affected by the weakness, are documented in the Affected Systems column. For example: SQL Server:master, or Http://127.0.0.1

Finding

A detailed description of the finding provides information on how the actual test results fail to meet the security and privacy requirement. The first line of this description with the date of the SAR is used to prepare the Plan of Action and Milestone(s) and provides easy reference to the SAR for additional information.

Failed Test Description

The column for Failed Test Description documents the control’s weakness that resulted in the finding. This description provides specific information from the security and privacy policy, requirements, guidance, test objective, or published industry best practices that was not provided with the controls implementation.

Actual Test Results

The Actual Test Results provide specific information on the observed failure of the test objective, policy, or guidance. This may also contain output from a test performed on the system revealing non-compliance.

Corrective Actions

The Corrective Actions column presents the recommended actions to resolve the vulnerability. The Auditor provides these suggestions to present guidance on a potential fix.

POA&M Reference

Identify the corresponding POA&M reference number.

Status

The Status column provides status information, which includes when the vulnerability was identified, actions being taken, or resolution of the weakness or vulnerability.

[Delete this instruction and all other instructions from your final version of this document.]

Complete Table 3. Add rows as necessary.

Table 3. Detailed Findings Table

Row #	Weakness	Risk Level	Control #	CIS Top 20 Control	OWASP Top 10	Affected Systems	Finding	Failed Test Description	Actual Test Results	Corrective Actions	POA&M Reference#	Status

Appendix A. Infrastructure Scan Results

Infrastructure scans include scans of operating systems, networks, routers, firewalls, domain name servers (DNS), domain servers, network information security (NIS) masters, and other devices that keep the network running. These scans can include both physical and virtual Host and devices. The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> infrastructure. <Number> percent of the inventory was scanned. For the remaining inventory, the Auditor performed a manual review of configuration files to analyze for existing vulnerabilities. Any findings found as the result of the scans were documented in the SAR’s Detail Findings Table (Table 3).

A.1 Infrastructure Scans: Raw Scan Results

Instruction: Provide all - infrastructure scan results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

[Delete this and all other instructions from your final version of this document.]

Table 4 lists the files that are included.

Table 4. Raw Scan Results by Infrastructure Scanner

Title of the Document	Description	File Name (Includes Extension)

A.2 Instructure Scans: False Positive Reports

Instruction: Use the summary table to identify false positives that were generated by the scanner. For each false positive reported, add an explanation as to why that finding is a false positive. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “IS” in the identifier number refers to “Infrastructure Scan.”

[Delete this and all other instructions from your final version of this document.]

Table 5 identifies false positives that were generated by the infrastructure scanner.

Table 5. False Positive Reports by Infrastructure Scanner

ID #	Page and IP Address	Scanner Severity Level	Finding	False Positive Explanation
1-FP-IS				
2-FP-IS				

Appendix B. Database Scan Results

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> databases. <Number> % percent of all databases were scanned.

B.1 Database Scans: Inventory of Databases Scanned

Instruction: Indicate the databases that were scanned. For "Function," indicate the function that the database plays for the system (e.g., database image for end-user development, database for authentication records). Add additional rows as necessary.

[Delete this and all other instructions from your final version of this document.]

Table 6 presents the database inventory scan results.

Table 6. Database Inventory Scan Results

IP Address	Hostname	Software / Version	Function	Comment

B.2 Database Scans: Raw Scan Results

Instruction: Provide all database scan results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

[Delete this and all other instructions from your final version of this document.]

Table 7 lists the files that are included.

Table 7. Raw Scan Results

Title of Document	Description	File Name (Includes Extension)

B.3 Database Scans: False Positive Reports

Instruction: Use the summary table to identify false positives that were generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “DS” in the identifier number refers to “Database Scan.”

[Delete this and all other instructions from your final version of this document.]

Table 8 identifies false positives that were generated by the database scanner.

Table 8. False Positives Generated by the Database Scanner

ID #	IP Address	Scanner Severity Level	Finding	False Positive Explanation
1-FP-DS				
2-FP-DS				
3-FP-DS				

Appendix C. Web Application Scan Results

The <Scanner Name, Vendor, & Version #> was used to scan the <Information System Abbreviation> web applications. <Number> % of all web applications was scanned.

Instruction: Indicate the web applications that were scanned. For “Function,” indicate the function that the web-facing application plays for the system (e.g., control panel to build virtual machines). Add additional rows as necessary.

[Delete this and all other instructions from your final version of this document.]

C.1 Web Applications Scans: Inventory of Web Applications Scanned

Table 9lists the web applications that were scanned and the function that the web-application performs for the system.

Table 9. Inventory of Web Applications Scanned

Login URL	IP Address of Login Host	Function	Comment

C.2 Web Applications Scans: Raw Scan Results

Instruction: Provide all web application scans results generated by the scanner in a readable format. Bundle all scan results into one zip file. Do not insert files that require a scan license to read the file.

[Delete this and all other instructions from your final version of this document.]

Table 10 lists the files that are included.

Table 10. Raw Scan Results

Title of Document	Description	File Name (Includes Extension)

C.3 Web Applications Scans: False Positive Reports

Instruction: Use the summary table to identify false positives that were generated by the scanner. Use a separate row for each false positive reported. If one IP address has multiple false positive reports, give each false positive its own row. For each false positive reported, add an explanation as to why that finding is a false positive. Add as many rows as necessary. The “FP” in the identifier number refers to “False Positive” and the “WS” in the identifier number refers to “Web Application Scan.”

[Delete this and all other instructions from your final version of this document.]

Table 11 identifies each false positive that was generated by the web applications scanner.

Table 11. False Positive Reports by Web Applications Scanner

ID #	IP Address	Scanner Severity Level	Finding	False Positive Explanation
1-FP-WS				
2-FP-WS				
3-FP-WS				

Appendix D. Penetration Test Report

Instruction: The results reported in this appendix should be components identified in Section 2 of the Security and Privacy Controls Assessment Test Plan and should include the OWASP Top 10 results specified in subsection 2.4.

[Delete this and all other instructions from your final version of this document.]

The scope of this assessment was limited to the <Information System Abbreviation> solution, including <List components here as documented in the Security and Privacy Test Plan Section 2 or > components. The Auditor conducted testing of <Acronym of EDE Entity> activities from the <Location > via an attributable Internet connection.

Table 12 provides IP addresses and uniform resource locators (URL) for all the in-scope systems at the beginning of the assessment.

Table 12. IP Addresses and URLs for In-Scope Systems

Application	IP/URL	OWASP Top 10	Penetration Test Results

Appendix E. Penetration Test and Scan Results Summary

Instruction: Summarize the scan assessment results in the following table. Ensure that the scanner severity level is appropriately mapped to the risk level ratings.

[Delete this and all other instructions from your final version of this document.]

Table 13 is a summary of all scan assessment results appropriately mapped to the risk level ratings.

Table 14. Summary of Scan Results

Risk Level	OS Scans	Web Scans	DB Scans	Source Code	Penetration Test	Total
High						
Moderate						
Low						
Total						

Table 15 summarizes the total risk findings.

Table 15. Total Risk Findings

Risk Level	Risks from Scan Testing	Total Risks
High	<#>	<#> (<#>% of Grand Total)
Moderate	<#>	<#> (<#>% of Grand Total)
Low	<#>	<#> (<#>% of Grand Total)
Total	<#>	<#>