OMB Control #: 0938-NEW
Expiration Date: XX/XX/20XX

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Centers for Medicare & Medicaid Services

INTERCONNECTION SECURITY AGREEMENT (ISA)
BETWEEN
CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
AND
ENHANCED DIRECT ENROLLMENT (EDE) ENTITY
<INSERT NON-CMS ORGANIZATION NAME>

ISA Version <Insert #>

<INSERT ISA Date>

Table of Contents

1. Introduction 1

2. CMS Background 2

2.1 CMS 2
2.2 CMS Information Security Program 2
2.3 CMS Roles and Responsibilities 2
2.3.1 CMS Chief Information Officer (CIO) 2
2.3.2 CMS Chief Information Security Officer (CISO) 2
2.3.3 CMS Senior Official for Privacy (SOP) 2
2.3.4 CMS Information System Security Officer (ISSO) 2
2.3.5 Center for Consumer Information and Insurance Oversight (CCIIO) 3
2.3.6 CMS Cyber Integration Center (CCIC) 3

3. Non-CMS Organization Background 3

3.1 Non-CMS Organization 3
3.2 IT Security Program 3
3.3 Roles and Responsibilities 3
3.3.1 <Role> 4
3.3.2 <Role> 4
3.3.3 <Role> 4
3.3.4 <Role> 4
3.3.5 <Role> 4

4. Scope 4

5. Authority 5

6. Statement of Requirements 5

6.1 General Information/Data Description 6
6.1.1 CMS Hub Description 6
6.1.2 Non-CMS Organization System Description 7
6.2 Services Offered 7
6.3 Security and Privacy Controls 7

7. Request to Connect 8

7.1 Required Documents 8

8. Security Responsibilities 8

8.1 Communication / Information Security Points of Contact 9
8.2 Responsible Parties 9

9. Personnel / User Security 9

9.1 User Community 9

9.2 Commitment to Protect Sensitive Information....10
9.3 Training and Awareness....10
9.4 Personnel Changes / De-Registration....11

10. Policies 11

10.1 Rules of Behavior....11
10.2 Security Documentation....11

11. Network Security 12

11.1 Network Management....12
11.2 Material Network Changes....12
11.3 New Interconnections....12
11.4 Network Inventory....13
11.5 Firewall Management....13
11.6 Penetration Test....13

12. Incident Prevention, Detection, and Response 14

12.1 Incident Handling....14
12.2 Intrusion Detection....15
12.3 Disasters and Other Contingencies....15

13. Notice 15

14. Modifications 16

15. Compliance 16

16. Termination 16

17. Cost Considerations 16

18. Timeline 17

19. Order of Precedence 17

20. Confidentiality 17

21. Survival 17

22. Records 18

23. Assignment and Severability 18

24. Warranty 18

25. Limitation of Liability 18

26. Force Majeure 19

27. Signatures 20

Appendix A. Responsible Parties 23

A.1 Authorizing Official 23
A.2 Other Designated Contacts 23
A.3 Assignment of Security and Privacy Responsibility 24

Appendix B. Primary EDE Entities Connection and Data Sharing with Upstream EDE Entities 26

B.1 Upstream EDE Entities Overview 26
B.2 Data Connections 27
B.3 Additional Functionality or Systems 29
B.4 Data Flow/Topological Diagram 32

List of Figures

Figure 1: EDE Data Flow Diagram 6
Figure 2. Data Flow/Topological Diagram 32

List of Tables

Table 1. System Authorizing Official 23
Table 2. Information System Management Point of Contact 24
Table 3. Information System Technical Point of Contact 24
Table 4. EDE Entity Name Internal ISSO (or Equivalent) Point of Contact 24
Table 5. EDE Entity Internal Official for Privacy (or Equivalent) Point of Contact 25
Table 6. CMS ISSO Point of Contact 25
Table 7. Upstream EDE Entity Overview 26
Table 8. Interconnections and Data Exchange Between EDE Environment Provider and Upstream Entities 28
Table 9. Additional Functionality or Systems 31

The following CMS and <Insert Non-CMS Organization Name> ISA Review Log is maintained to record the annual reviews.

Record of Changes

Version	Date	Author / Owner	Description of Change	CR #
<Insert ISA Version Reviewed>	<Insert Date of the Review>	<Insert Staff Name of the Reviewer>, <Insert Staff Reviewer's Organization>		

CR: Change Request

1. Introduction

The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and the Enhanced Direct Enrollment (EDE) Entity,[1] <Insert Non-CMS Organization Name> (hereafter referenced as the "Non-CMS Organization"), regarding the development, management, operation, and security of a connection between CMS's Data Service Hub (Hub) (hereafter known as the CMS Network) and the Non-CMS Organization's network. This ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of CMS information[2] as well as the information that is owned by the external organization that has a network interconnection[3] with CMS. This ISA ensures the adequate security[4] of CMS information being accessed and provides that all network access satisfies the mission requirements of both CMS and the Non-CMS Organization (hereafter referenced as "both parties").

Federal policy requires agencies to develop ISAs for federal information systems and networks that share or exchange information with external information systems and networks. This ISA is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Rev. 1, *Managing the Security of Information Exchanges,*[5] and shall comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, *Privacy or Security Safeguards*. The guidelines establish information security (IS) measures that shall be taken to protect the connected systems and networks and shared data. CMS Information Technology (IT) managers and IS personnel shall comply with the NIST guidelines in managing the process of interconnecting information systems and networks.

This ISA documents interconnection arrangements and IS responsibilities for both parties, outlines security safeguards, and provides the technical and operational security requirements. This ISA also specifies business and legal requirements for the information systems and networks being interconnected. This ISA authorizes mutual permission to connect both parties and establishes a commitment to protect data that is exchanged between the networks or processed and stored on systems that reside on the networks. Through this ISA, both parties shall minimize the susceptibility of their connected systems and networks to IS risks and aid in mitigation and recovery from IS incidents.

---

1 EDE Entities are considered Non-Exchange Entities (NEE) and, as such, are required to comply with the privacy and security standards that are at least as protective as the standards the Exchange has established and implemented for itself.

2 "Information" is defined as "any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government." (Executive Order 12958)

3 "Network interconnection" is defined as the primary "direct connection of two or more IT networks for the purpose of sharing data and other information resources." (This is based on the definition of system interconnection in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems.*)

4 "Adequate security" is defined as "a level of security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information." (Office of Management and Budget [OMB] Circular A-130)

5 Located at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf.

2. CMS Background

2.1 CMS

As an Operating Division of the Department of Health and Human Services (HHS), CMS administers Medicare, Medicaid, Children's Health Insurance Program (CHIP), as well as programs created under the Patient Protection and Affordable Care Act (PPACA) of 2010, including the Health Insurance Exchange program. It is CMS's mission to ensure effective, up-to-date health care coverage and to promote quality care for beneficiaries.

2.2 CMS Information Security Program

The CMS IS Program helps CMS accomplish its mission by ensuring the CIA of CMS information resources. The CMS IS Program has developed policies, standards, procedures, and guidelines that ensure the adequate protection of agency information and comply with federal laws and regulations. CMS monitors the security of its network twenty-four (24) hours a day, seven (7) days a week (i.e., 24/7) through various management, operational, and technical processes. Training initiatives are continuously updated to ensure that managers, users, and technical personnel are aware that they are responsible for the adequate security of their information systems.

2.3 CMS Roles and Responsibilities

2.3.1 CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the overall implementation and administration of the CMS Information Security and Privacy Program.

2.3.2 CMS Chief Information Security Officer (CISO)

The CMS CISO supports the CMS CIO in the implementation of the CMS Information Security Program. The CMS CISO directs, coordinates, and evaluates CMS's Information Security policy. The CISO collaborates with the CMS Senior Official for Privacy to carry out Information Security and Privacy responsibilities.

2.3.3 CMS Senior Official for Privacy (SOP)

The CMS SOP carries out the CIO's privacy responsibilities under federal requirements in conjunction with the CISO. The CMS SOP leads CMS privacy programs and promotes proper information security and privacy practices and is responsible for the development and implementation of privacy policies and procedures.

2.3.4 CMS Information System Security Officer (ISSO)

The CMS ISSO is the liaison for IS within their assigned area of responsibility. ISSOs implement standard IS policies and collaborate across CMS concerning the CIA of information resources. Although the ISSOs report directly to their own management, they have responsibilities to the CMS CISO as part of their IS responsibilities, and therefore, to the CMS

CIO. In their IS role, ISSOs take direction from the CMS CIO or the CMS CISO when action is required to protect CMS assets from potential vulnerabilities and threats. The CMS CISO and ISSOs will work with Non-CMS Organization to enhance IS measures.

2.3.5 Center for Consumer Information and Insurance Oversight (CCIIO)

The CCIIO, as the CMS Business Owner (BO), is responsible for the management and oversight of CMS's Health Insurance Exchange Hub system, which is the CMS information system that requires the interconnection with the Non-CMS Organization. The BO serves as the primary point of contact (POC) for the CMS information system.

2.3.6 CMS Cyber Integration Center (CCIC)

The CCIC monitors the security of the CMS information system 24/7 using the expertise of Information Technology (IT) security professionals and automated IS processes. The CCIC identifies IS incidents, characterizes the nature and severity of incidents, and provides immediate diagnostic and corrective actions when appropriate. CCIC members are trained in investigating IS events such as web defacements, computer compromises, and viruses. The CCIC continuously enhances its IS auditing methods as well as incident handling procedures to respond to the growing demands of IS.

3. Non-CMS Organization Background

3.1 Non-CMS Organization

Instruction: Insert background information about the Organization, including a brief description of the organization and its mission, as well as the business needs as it relates to the interconnection with the CMS Hub. Please update the Table of Contents once all insertions to the document are complete. **[Delete this instruction.]**

[Click here and type text here]

3.2 IT Security Program

Instruction: Insert a brief description of the overall Organization IT security program and include the references to the interconnection with the CMS Hub. **[Delete this instruction.]**

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

3.3 Roles and Responsibilities

Instruction: <Insert a brief description of each role and associated responsibilities of the Non-CMS Organization that are equivalent to the CMS roles and responsible for implementing IT and IS policies, procedures, and tools that support CIA. Add or delete additional Roles as needed.> **[Delete this instruction.]**

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

3.3.1 <Role>

Instruction: Insert roles and responsibilities. **[Delete this instruction.]**

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

3.3.2 <Role>

Instruction: Insert roles and responsibilities. **[Delete this instruction.]**

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

3.3.3 <Role>

Instruction: Insert roles and responsibilities. **[Delete this instruction.]**

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

3.3.4 <Role>

Instruction: Insert roles and responsibilities. **[Delete this instruction.]**

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

3.3.5 <Role>

Instruction: Insert roles and responsibilities. **[Delete this instruction.]**

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

4. Scope

Instructions: The styles for bulleted text are as follows:

- For bullet lists where any one of the bullets extends beyond one line of text, use "Bullet List Multiple." The last bullet in the list is styled as "Bullet List Multiple Last," which adds spacing after the bullet and before the ensuing paragraph.
- For bullet lists that only have single lines of text, use "Bullet List Single" and "Bullet List Single Last," respectively.

Note: To provide the second and third level of indenture for bullets, simply hit <Tab> after you have established the next bullet in the list. To achieve the third level of indenture after the second, simply hit a second <Tab>, as follows:

- Text for initial bullet in series
  - Tab 1 for second level
    - Tab 2 for third level **[Delete these instructions.]**

The scope of this ISA is based on, but is not limited to, the following activities, users, and components:

- Interconnection between a CMS information system(s) and the Non-CMS Organization.

- Existing and future users, including employees from both parties, contractors, and subcontractors at any tier; and other federally and non-federally funded users managing, engineering, accessing, or utilizing the Non-CMS Organization Network.
- Related network components belonging to both parties, such as hosts, routers, and switches; IT devices that assist in managing security such as firewalls, intrusion detection systems (IDS), and vulnerability scanning tools; desktop workstations; servers; and major applications (MA) that are associated with the network connection between both parties.[6]

5. Authority

By connecting with the CMS network and CMS information system, Non-CMS Organization agrees to be bound by this ISA and use the CMS Network and CMS information system(s) in compliance with this ISA.

The authority for this ISA is based on, but not limited to, the following, if and to the extent applicable:

- Federal Information Security Modernization 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 1996, P.L. 104-191;
- 45 C.F.R. § 155.260 Privacy and Security of Personally Identifiable Information;
- 45 C.F.R. § 155.280 Oversight and Monitoring of Privacy and Security Requirements; and
- Patient Protection and Affordable Care Act of 2010.

This ISA is also in compliance with HHS policies[7] and CMS policies listed at the CMS IS webpage.[8]

6. Statement of Requirements

The expected benefit of the interconnection is <Insert a detailed Non-CMS Organization Business Expectation>.

[6] A "major application" is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (OMB A-130)

[7] Located at: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html.

[8] Located at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/.

6.1 General Information/Data Description

6.1.1 CMS Hub Description

All communication with the Hub is facilitated via Web services over the Internet. The Hub conveys information, using Transport Layer Security (TLS), version 1.2 for data encryption, server authentication, and message integrity. It uses Public Key Infrastructure (PKI) to authenticate connections. To protect the confidentiality of data transmitted from one system to another system, messages are encrypted, using the Hypertext Transfer Protocol Secure (HTTPS) protocol.

All Application Programming Interface (API) transactions provided by an EDE Entity will go through the Hub for confirmation that the requesting EDE Entity is authorized by CMS. Upon confirmation, the API request will be passed to the Federally-facilitated Exchange (FFE), at which point the FFE will validate the API request. The groups of services depicted in Figure 1 enable the FFE to provide internal and external stakeholders with the following capabilities:

- **Marketplace Consumer Record (MCR) APIs:** Enable the Exchange to provide customer-related data and search capabilities.
- **Standalone Eligibility Service (SES) APIs:** Enable the Exchange to determine the customer's eligibility for Qualified Health Plans (QHP) and /or Qualified Dental Plans (QDP) and associated subsidies.
- **Issuer and Enrollment Services (IES) APIs:** Enable the Exchange to provide data to redirect consumers to the issuer payment portal.
- **Document Storage and Retrieval Service (DSRS) APIs:** Enable the Exchange to provide document upload and retrieval of Exchange-generated notices.
- **Eligibility and Enrollment (EE) APIs:** Enable the Exchange to provide enrollment generation capabilities.

Figure 1 is a high-level topological diagram illustrating the interconnectivity between the Hub and EDE entity systems.

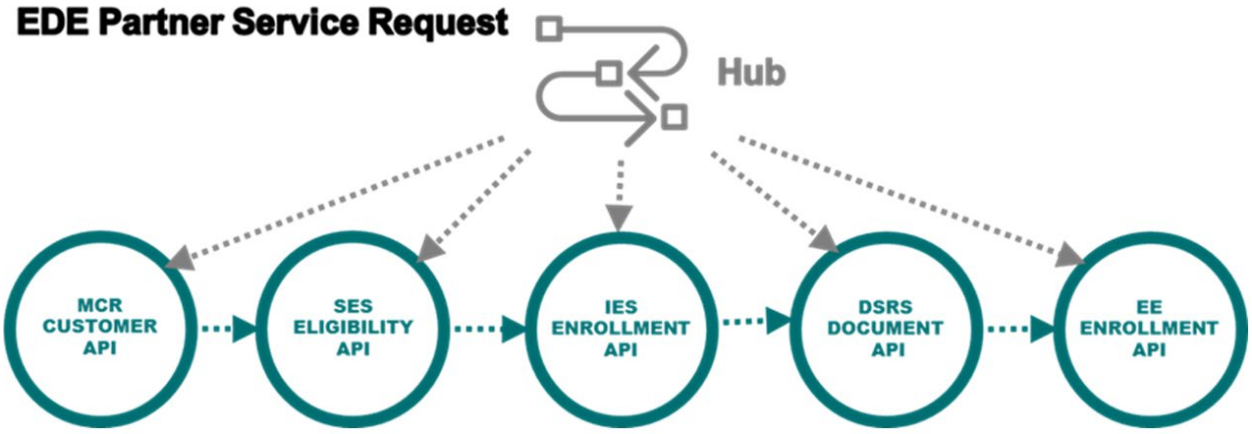

Figure 1: EDE Data Flow Diagram

6.1.2 Non-CMS Organization System Description

Instruction: Insert high-level Non-CMS Organization description of the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems / networks. Non-CMS Organization, Primary EDE Entity, must complete Appendix B. The description should also include the method of interconnection to the Hub.

Include a Topological Diagram of the system which depicts the interconnectivity between the Hub and the Non-CMS Organization including all components (i.e., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations) and interfaces (i.e., real-time, on-demand, and batch) on which data and information is exchanged. Ensure the information system's name/acronym is documented in the diagram.

To insert a figure object, style the insertion point as "Figure" and paste the object as a Picture (Enhanced Metafile) or .png. After inserting the object, hit the hard return and insert a figure caption (styled as "Figure Caption" following the figure. By contrast, insert table captions (styled as "Table Caption" before an inserted table. [**Delete this instruction.]**

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

6.2 Services Offered

CMS shall:

- Provide 24/7 operation of the CMS IT Service Desk (1-800-562-1963, 410-786-2580, or cms_it_service_desk@cms.hhs.gov) for the Non-CMS Organization POC to communicate any security issues; and
- Provide installation, configuration, and maintenance of CMS edge router(s) with interfaces to multiple CMS core and edge routers.

The Non-CMS Organization shall:

Instruction: Insert non-CMS Organization IT Help Desk information regarding operating times, process, and contact information. **[Delete this instruction.]**

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

6.3 Security and Privacy Controls

CMS shall:

- Comply with the latest *CMS Acceptable Risk Safeguards (ARS)*[9], which are based on the most recent NIST SP 800-53 and HHS policy and standards.

The Non-CMS Organization shall:

[9] The *CMS Acceptable Risk Safeguards (ARS)* is located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.

- Adhere to the security and privacy requirements specified in the *Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP)* document,[10] which are specifically incorporated herein.

7. Request to Connect

The Non-CMS Organization sends to CMS a completed ISA document and artifacts of compliance with security and privacy control requirements. After review of the ISA, along with all required artifacts and an evaluation of risk, the CMS CIO, or his designee, will act on the request to connect to the Hub in writing by signing the ISA or by denying the request. No PII shall pass through any CMS network before the Non-CMS Organization obtains a fully signed ISA.

The Non-CMS Organization must also send to CMS a signed EDE Agreement and meet all requirements set forth in that Agreement before CMS will permit connection to the Hub.

7.1 Required Documents

Pursuant to 45 C.F.R. § 155.260, Privacy and Security of Personally Identifiable Information, and 45 C.F.R. § 155.280, Oversight and Monitoring of Privacy and Security Requirements, the Non-CMS Organization shall report, on a continuing basis, the status of their security posture to Non- CMS Organization's authorizing official and CMS. If the Non-CMS Organization does not meet the required reporting timeframes, the ISA may be revoked. Before CMS can make a risk-based decision on the system's ISA, the following agreements and compliance artifacts are required:

1. EDE Agreement;
2. Interconnection Security Agreement (ISA), renewed every year or whenever there is a major change;
3. Security Assessment Report (SAR), performed by an auditor, and Plan of Action & Milestones (POA&M); and
4. Information Security and Privacy Continuous Monitoring (ISCM)[11] artifacts.

8. Security Responsibilities

Both parties shall:

- Maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels.

[10] The *Non-Exchange Entity System Security and Plan (SSP)* is located at: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

[11] The *Non-Exchange Entity (NEE) Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide* is located at: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

- Non-CMS Organization's responsibilities under this provision are in addition to those specified in Section 6.3.

8.1 Communication / Information Security Points of Contact

Both parties shall:

- Designate a technical lead for their respective network and provide POC information to facilitate direct contacts between technical leads of each party to support the management and operation of the interconnection;
- Maintain open lines of communication between POCs at both the managerial and technical levels to ensure the successful management and operation of the interconnection; and
- Inform their counterpart promptly of any change in technical POCs and interconnections.

CMS shall:

- Ensure its staff informs their counterparts at the Non-CMS Organization promptly of any change in technical POC and interconnection; and
- Identify a CMS ISSO to serve as a liaison between CMS and the Non-CMS Organization and assist the Non-CMS Organization in ensuring that its IS controls meet or exceed CMS requirements.

The Non-CMS Organization shall:

- Designate an IS POC, the equivalent of the CMS ISSO, who shall act on behalf of the Non-CMS Organization and communicate all IS issues involving the Non-CMS Organization to CMS via the CMS ISSO.

8.2 Responsible Parties

Appendix A is a list of the responsible parties for each system. Appendix A will be updated whenever necessary. Updating Appendix A does not require either party to re-sign this ISA. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix A and to notify the alternate party of such changes; each party will use reasonable efforts to do so within thirty (30) days of any material personnel change.

9. Personnel / User Security

9.1 User Community

Both parties shall:

- Ensure that all employees, contractors, and other authorized users with access to the CMS Network and the Non-CMS Organization as well as the data sent and received from either organization are not security risks and meet the personnel security / suitability

requirements of the *CMS Business Partners System Security Manual* (2018)[12] as a guide, which is specifically incorporated herein.

The Non-CMS Organization shall:

- Enforce the following IS best practices:
  - **Least Privilege –** Only authorizing access to the minimal amount of resources required for a function;
  - **Separation of Duties –** A security method that manages conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual; and
  - **Role-Based Security –** Access controls to perform certain operations ("permissions") are assigned to specific roles.

9.2 Commitment to Protect Sensitive Information

Both parties shall:

- Not release, publish, or disclose information to unauthorized personnel, and shall protect such information in accordance with this ISA, the EDE Agreement, and any other pertinent laws and regulations governing the responsibility to adequately safeguard federal agency systems.

The Non-CMS Organization shall:

- Require that its employees and contractors comply with the security requirements set forth in this ISA, EDE Agreement, and the organization's specific information security policies, standards, and procedures.
- Require that outsourced operations where non-CMS personnel may have access to information, CMS systems, and network components comply with requirements of Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards, and CMS IS policies, standards, and procedures, which are specifically incorporated herein.

9.3 Training and Awareness

Both parties shall:

- Have all users, including employees, contractors, and other authorized users, complete the information security and privacy awareness training on execution of this ISA and then annually thereafter; and
- Train, monitor, and audit staff on requirements related to the authorized use and sharing of PII with third parties, and on the consequences of unauthorized use or sharing of PII.

[12] The *CMS Business Partners System Security Manual* is located at: http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/117_systems_security.pdf.

9.4 Personnel Changes / De-Registration

Both parties shall:

- Provide notification to their respective BOs of the separation or long-term absence of their network owner or technical lead; and
- Provide notification to their respective BO of any changes in the ISSO or POC information.

10. Policies

10.1 Rules of Behavior

CMS shall:

- Ensure that all CMS system users with access to the CMS Network shall adhere to all current *HHS Rules of Behavior*.[13]

The Non-CMS Organization shall:

- Require that all users with access to the Non-CMS Organization's system and its connection with the Hub, adhere to the terms of this ISA and the EDE Agreement executed between the Non-CMS Organization and CMS.
- Require the Non-CMS Organization's Rules of Behavior provide protections that are commensurate with current *HHS Rules of Behavior*.

10.2 Security Documentation

Both parties shall:

- Ensure that security is planned for, documented, and integrated into the System Life Cycle from the IT system's initiation to the system's disposal. For applicable guidance, please refer to CMS Target Life Cycle[14] and the *CMS Risk Management Handbook*.[15]

CMS shall:

- Review the CMS System Security and Privacy Plan (SSP) for CMS information systems and the CMS network annually and update it when a major modification occurs, as required by the CMS SSP Procedures.

[13] Located at: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/rules-of-behavior-for-use-of-hhs-information-resources/index.html.

[14] Located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/TLC.

[15] Located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.

The Non-CMS Organization shall:

- Maintain an SSP based on the *Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP)* document[16] on the Non-CMS Organization's network and update annually or whenever there is a significant change;[17] and
- Make accessible to CMS all IS program documents including, but not limited to, those documents specified in Section 7.1.

11. Network Security

11.1 Network Management

Both parties shall:

- Ensure that this interconnection is isolated from all other customer / business processes to the greatest extent possible.

11.2 Material Network Changes

Both parties shall:

- Submit to the CMS CCIIO any proposed material changes to either network or the connecting medium accompanied by a valid business justification;
- Renegotiate this ISA before any material changes are implemented;
- Report planned technical changes to the network architecture that affect the interconnection to the CMS CCIIO Hub team;
- Conduct a risk assessment based on the new network architecture and modify and re-sign this ISA within one (1) month prior to implementation; and
- Notify the CMS CCIIO Hub team when access is no longer required.

11.3 New Interconnections

The Non-CMS Organization shall:

- List and define any new interconnections or updates to any existing interconnections, including any new updates in processes related to sharing, utilizing, and downloading data; and

[16] The *Non-Exchange Entity System Security and Plan (SSP)* is located at: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

[17] Per NIST 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.

- Notify CMS when new interconnections impact the security posture of the EDE Pathway or the Hub, unless expressly agreed in a modification to the relevant ISA and signed by both parties.

11.4 Network Inventory

The Non-CMS Organization shall:

- Maintain and make available to CMS on request a list of all Non-CMS Organization subnets connected to CMS's network, if applicable, and periodically update the information, including information on each owner, physical location, Internet Protocol (IP) address, host's name, hardware, operating system version, and applications.

11.5 Firewall Management

CMS shall:

- Configure the CMS network perimeter firewall in accordance with CMS IS policy;
- Block all network traffic incoming from the Internet to CMS unless it is explicitly permitted; and
- Install a firewall between the perimeter (demarcation point) of the Non-CMS Organization's network and CMS's network if deemed necessary by CMS CCIIO Hub team.

The Non-CMS Organization shall:

- Maintain responsibility for configuring all Non-CMS Organization network perimeter firewalls in accordance with a policy at least as stringent as CMS IS policy as reflected in this ISA; and
- Provide to the CMS CCIIO Hub team a list of Non-CMS Organization authorized web HTTP, File Transfer Protocol (FTP), and Simple Mail Transport Protocol (SMTP) servers (identified individually as HTTP, FTP, and/or SMTP) on the Non-CMS Organization's network.

11.6 Penetration Test

The Non-CMS Organization shall:

- Execute a Rules of Engagement with their penetration testing team;
- Not target IP addresses used for the CMS and Non-CMS Organization connection;
- Conduct penetration testing in the lower environment that mirrors the production environment;
- Not conduct penetration testing in the production environment;
- Notify CMS designated technical counterparts on their annual penetration testing schedule; and

- Provide the following information to CMS a minimum of 5 business days prior to initiation of testing:
  - Period of testing performance (specific times for all testing should be contained in individual test plans);
  - Target environment resources to be tested (IP addresses, Hostname, URL); and
  - Any restricted hosts, systems, or subnets that are not to be tested.

12. Incident Prevention, Detection, and Response

12.1 Incident Handling

CMS shall:

- Handle and report incidents in accordance with the *CMS Risk Management Handbook (RMH) Chapter 08: Incident Response*.[18]

The Non-CMS Organization shall:

- Implement Breach and Incident Handling procedures that are consistent with CMS's Incident and Breach Notification Procedures and incorporate these procedures in the Non-CMS Organization's own written policies and procedures.
- Implement specifications. Such policies and procedures would:
  - Identify the Non-CMS Organization's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents[19] or Breaches[20];
  - Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes;[21] and

---

18 Located at the CMS IS webpage, available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response.

19 OMB Memorandum M-17-12 defines "incident" or "security incident" as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. OMB Memorandum M-17-12, Preparing for or Responding to A Breach of Personally Identifiable Information, January 3, 2017. Located at: http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf.

20 OMB Memorandum M-17-12 defines "breach" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.

21 Please refer to *RMH Chapter 08 Incident Response Appendix K - Incident Report Template* located at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template.

- Require reporting any 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 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

12.2 Intrusion Detection

Both parties shall:

- Monitor intrusion detection activities and disseminate intrusion detection alerts to their respective BO counterparts for all networks within the scope of this ISA[22];
- Report to both CMS and the Non-CMS Organization's BO any security incident that occurs on either organization's network within the scope of this ISA; and
- Block inbound and outbound access for any CMS or Non-CMS Organization information systems on the network within the scope of this ISA that are the source of unauthorized access attempts, or the subject of any security events, until the risk is remediated.

12.3 Disasters and Other Contingencies

Both parties shall:

- Promptly notify their designated counterparts as defined in the information system contingency plan in the event of a disaster or other contingency that disrupts the normal operation of one or both connected networks.

13. Notice

Both parties shall:

- Provide notice to all persons specifically required under this ISA in writing and shall be delivered as follows:

If to Non-CMS Organization:

<Insert Non-CMS Organization mailing address>

If to CMS:

Centers for Medicare & Medicaid Services (CMS)
Center for Consumer Information & Insurance Oversight (CCIIO)
Room 739H 200 Independence Avenue, SW
Washington, DC 20201

Notices sent by hand or overnight courier service, or mailed by certified or registered mail, shall be deemed to have been given when received, provided that notices not given on a business day

[22] Intrusion detection audit logs must be kept for purposes of forensic investigation in the case of an incident.

(i.e., Monday – Friday excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. Either party to this Agreement may change its contact information for notices and other communications by providing thirty (30) days' written notice of such change in accordance with this provision.

14. Modifications

If any personnel changes occur involving the POCs listed in this ISA, the terms of this ISA shall remain in full force and effect, unless formally modified by both parties. Any modifications that materially change the security posture of the portion of the information system related to this ISA shall be in writing and agreed and approved in writing by both parties.

15. Compliance

Non-compliance with the terms of this ISA by either party or unmitigated security risks in violation of this ISA may lead to termination of the interconnection. CMS may block network access for the Non-CMS Organization if the Non-CMS Organization does not implement reasonable precautions to prevent the risk of security incidents spreading to CMS's network. CMS is authorized to audit the security of Non-CMS Organization's Network periodically by requesting that Non-CMS Organization provide documentation of compliance with the security requirements in this ISA (please refer to Section 22, Records). The Non-CMS Organization shall provide CMS reasonable access to its IT resources impacted by this ISA for the purposes of audits, subject to applicable legal requirements and policies.

16. Termination

Termination of this ISA will result in termination of the functionality and electronic interconnection(s) covered by this ISA. The termination of EDE Agreement and/or Issuer Agreement and/or Web-broker Agreement will result in termination of this ISA. Termination of any of the agreements referenced in this provision will result in termination of DE Entity's ability of to use the EDE Pathway as allowed by this ISA.

17. Cost Considerations

Both parties agree to be responsible for their own systems and costs of the interconnecting mechanism and/or media. No financial commitments to reimburse the other party shall be made without the written concurrence of both parties. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system/network owners' organization. This ISA neither authorizes, requires, nor precludes any transfer of funds without the agreement of both parties.

18. Timeline

This Agreement becomes effective on the date the last of the two parties executes this Agreement and ends the day before the first day of the annual open enrollment period (OEP) for the benefit year beginning January 1, 2024.

19. Order of Precedence

In the event of an inconsistency between the terms and conditions of this ISA and the terms and conditions of any other agreement, memorandum of understanding, or acquisition between CMS and Non-CMS Organization, the terms and conditions of the EDE Agreement shall have precedence over this ISA. If the terms and conditions at issue are not otherwise covered in the EDE Agreement, the parties agree that the ISA will have precedence.

20. Confidentiality

Subject to applicable statutes and regulations, including the Freedom of Information Act, the parties agree that the terms and conditions (any proprietary information) of this ISA shall not be disclosed to any third party outside of the Government without the prior written consent of the other party.

Both parties may disclose the terms, conditions, and content of this ISA as reasonably necessary to their respective auditors, counsel, and other oversight agencies to respond to a properly authorized civil, criminal judicial process or regulatory investigation or subpoena or summons, issued by a federal or state authority having jurisdiction over either party for examination, compliance, or other purposes, as authorized by law. Any such disclosure may only be made after giving prior notice to the other party of the potential disclosure as soon as reasonably practical before such disclosure is required to be made. Either party, as a condition of its consent to disclosure, may require the other party to take sufficient measures to protect against the disclosure of information that could present significant risk to the security posture of the parties' systems, including the exposure of vectors of attack. Such measures include, but are not limited to, obtaining a protective order from a court of competent jurisdiction, disclosing the ISA in redacted form, or disclosing the ISA subject to a non-disclosure agreement, as appropriate under the circumstances and applicable law.

21. Survival

The Non-CMS Organization's duty to protect and maintain the privacy and security of PII, as well as the confidentiality requirements under Section 20, shall survive the termination of this ISA.

22. Records

The Non-CMS Organization shall maintain all records that it may create in the normal course of its business in connection with activity under this ISA for the term of this ISA and for at least ten (10) years after the date this ISA terminates or expires in accordance with 45 C.F.R. §§ 155.220(c)(3)(i)(E) or 156.705(c), as applicable. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this ISA. The records shall be made available during regular business hours at Non-CMS Organization offices, and CMS's review shall not interfere unreasonably with the Non-CMS Organization business activities.

23. Assignment and Severability

This ISA may not be assigned to another party without the specific written consent of the other party. If any term or condition of this ISA becomes inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the term or condition in question inoperative or unenforceable in any other case or circumstances, or of rendering any other term or condition contained in this ISA to be invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of a term or condition of this ISA shall not affect the remaining terms and conditions of this ISA.

24. Warranty

CMS does not warrant that Non-CMS Organization interconnection to the CMS network under this ISA will meet Non-CMS Organization requirements, expectations, or even the stated expected benefit of Non-CMS Organization interconnection to CMS (please refer to Provision 6, Statement of Requirements). Non-CMS Organization bears the entire risk regarding the quality and performance of its interconnection with the CMS, and Non-CMS Organization's exclusive remedy is to terminate this ISA in accordance with the terms and conditions herein.

CMS EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH REGARD TO NON-ORGANIZATION'S INTERCONNECTION TO THE CMS.

25. Limitation of Liability

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL CMS BE LIABLE TO NON-CMS ORGANIZATION OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER

COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

26. Force Majeure

Non-CMS Organization's failure to comply with any term or condition of this ISA as a result of conditions beyond its fault, negligence, or reasonable control (such as, but not limited to, war, strikes, floods, governmental restrictions, riots, fire, other natural disasters, or similar causes beyond Non-CMS Organization control) shall not be deemed a breach of this ISA.

27. Signatures

Both parties agree to work together to ensure the joint security of the connected networks and the data they store, process, and transmit, as specified in this ISA. Each party certifies that its respective network is designed, managed, and operated in compliance with this ISA, and all relevant federal laws, regulations, policies and the EDE System Security and Privacy Plan document. Each party attests that the information provided in this ISA is true, correct, and complete to the best of their knowledge. Each party also certifies that its respective network has been certified and accredited in accordance with NIST guidance.

By signing below, the parties agree to the terms and conditions of this ISA.

This "CMS INTERCONNECTION SECURITY AGREEMENT (ISA) BETWEEN CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) AND ENHANCED DIRECT ENROLLMENT ENTITY" has been signed and executed by:

FOR EDE ENTITY

The undersigned is an authorized official of EDE Entity who is authorized to represent and bind EDE Entity for purposes of this ISA.

Authorized Official for
<Insert Non-CMS Organization Name>

(Signature) (Date)
<Name and Title of Authorized Official of EDE Entity>

<Insert Non-CMS Organization Name>
<Non-CMS Organization Address>

<Non-CMS Organization Contact Number>

Chief Information Security Officer / Senior Officer of Privacy (equivalent) for
<Insert Non-CMS Organization Name>

(Signature) (Date)
<Name and Title>

FOR CMS

The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this ISA.

(Signature) (Date)

Kevin Allen Dorsey
Senior Information Security Officer
Center for Consumer Information and Insurance Oversight (CCIIO)
Centers for Medicare & Medicaid Services (CMS)

(Signature) (Date)

Marc Richardson
Director of Marketplace Information Technology Group (MITG)
Center for Consumer Information and Insurance Oversight (CCIIO)
Centers for Medicare & Medicaid Services (CMS)

(Signature) (Date)

Jeffrey D. Grant
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight (CCIIO)
Centers for Medicare & Medicaid Services (CMS)

(Signature) (Date)

Robert Wood
Director Information Security and Privacy Group (ISPG)
Chief Information Security Officer (CISO)
Office of Information Technology (OIT)
Centers for Medicare & Medicaid Services (CMS)

_____
(Signature) (Date)

George C. Hoffmann
Deputy Chief Information Officer (Dep. CIO)
Office of Information Technology (OIT)
Centers for Medicare & Medicaid Services (CMS)

_____
(Signature) (Date)

Appendix A. Responsible Parties

Instruction: Appendix A is a list of the responsible parties for each system. Appendix A will be updated whenever necessary. Updating Appendix A does not require either party to re-sign this ISA. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix A and to notify the alternate party of such changes; each party will use reasonable efforts to do so within thirty (30) days of any material personnel change. **[Delete this instruction.]**

[Click here and type text here]

A.1 Authorizing Official

Instruction: The Authorizing Official is the official designated by the EDE Entity organization, which is responsible for the security and privacy of this system. **[Delete this instruction.]**

[Click here and type text here]

Table 1. System Authorizing Official

System Authorizing Official Information	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

A.2 Other Designated Contacts

Instruction: AOs should use the following section to identify points of contact who understand the technical implementations of the identified system. Add more tables as needed.

Note: If you add more tables, be sure to update the Table Caption field to ensure the correct, sequential table numbering; update the cross-reference fields for the tables; and update the List of Tables in the front matter. If you copy a table, paste it at an insertion point styled as "Normal" and use the following command: Paste/Paste Special/Formatted Text (RTF) where Track Changes is turned off. **[Delete these instructions.]**

Table 2 and Table 3 identify the following individual(s) who possess in-depth knowledge of this system and/or its functions and operation.

Table 2. Information System Management Point of Contact

Information System Management POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 3. Information System Technical Point of Contact

Technical POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

A.3 Assignment of Security and Privacy Responsibility

The EDE Entity Information System Security Officer (ISSO) or equivalent, identified in Table 4, has been appointed in writing and is deemed to have significant cyber and operational role responsibilities.

Table 4. EDE Entity Name Internal ISSO (or Equivalent) Point of Contact

EDE Internal ISSO	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

The EDE Entity Information System Official for Privacy, identified in Table 5, has been appointed in writing and is deemed to have significant privacy operational role responsibilities.

Table 5. EDE Entity Internal Official for Privacy (or Equivalent) Point of Contact

EDE Internal Official for Privacy POC	Detail
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6 names the CMS Information System Security Officer responsible for providing assistance to the EDE Entity security and privacy officers.

Table 6. CMS ISSO Point of Contact

CMS ISSO POC	Detail
Name	CMS ISSOs
Title	ISSO
Company / Organization	CMS/Center for Consumer Information and Insurance Oversight/Marketplace IT Group
Address	7500 Security Blvd., Baltimore, MD 21244-1850
Email Address	directenrollment@cms.hhs.gov

Appendix B. Primary EDE Entities Connection and Data Sharing with Upstream EDE Entities

Instruction: Appendix B is a description of the data connections, functionality, and systems between a primary EDE Entity and its upstream EDE Entities. Primary EDE Entities will need to complete this form (all sections: B.1 through B.4) annually and when onboarding a new upstream EDE Entity as part of the Interconnection Security Agreement (ISA) and Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide. Updating Appendix B does not require the re-signing of the ISA by either party. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix B and for the notification of such changes to the alternate party within thirty (30) days of any personnel change.

A primary EDE Entity must complete this Appendix and return it via the CCC-SFTP to CMS. Please contact DE Support (directenrollment@cms.hhs.gov) with any questions. **[Delete this instruction.]**

B.1 Upstream EDE Entities Overview

Instructions: Populate Table 7 for each upstream EDE Entity, regardless of the upstream EDE Entity's current go-live status (i.e., live or onboarding). **[Delete this instruction.]**

Table 7 contains the following fields:

- **Upstream EDE Entity:** Document all known or unexpected EDE Entities and/or system name (if applicable).
- **Entity Type:** Document the Entity Type (e.g., issuer, web-broker, agent/broker).[23]
- **Partner ID(s):** Provide the Partner ID(s) for the upstream EDE Entity.

Table 7. Upstream EDE Entity Overview

Upstream EDE Entity	Entity Type	Partner ID(s)

[23] Definitions of each entity type are available in 45 C.F.R. § 155.20.

B.2 Data Connections

Instructions: During the annual EDE Agreement Renewal submission of the ISA, Primary EDE Entities must document all approved upstream EDE Entity relationships in Table 8. After the annual EDE Agreement Renewal submission, primary EDE Entities must submit a new Table 8 documenting each new upstream EDE Entity relationship.

Note: If you insert a new Table 8, be sure to update the Table Caption field to ensure the correct, sequential table numbering; update the cross-reference fields for the tables; and update the List of Tables in the front matter. If you copy a table, paste it at an insertion point styled as "Normal" and use the following command: Paste/Paste Special/Formatted Text (RTF) where Track Changes is turned off. **[Delete these instructions.]**

Note: A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems process including performing a Security Impact Analysis (SIA), a Business Impact Analysis (BIA), and potentially updating the 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. **[Delete this instruction.]**

Table 8 contains the following fields:

- **ID:** Unique identifier for the row item to track items between Table 8 and Table 9, as applicable.
- **Information System Name:** IT system environment name for the EDE Environment Provider.
- **Upstream EDE Entity Organization Name:** Document all known or expected upstream entities and/or system name (if applicable).
- **Information Being Transmitted:** For example, personally identifiable information (PII) data elements, enrollment information, eligibility information, and 834s.
- **Data Sharing Agreement in Place:** Briefly describe terms of the Agreement (e.g., Memorandum of Understanding [MOU)] and Business Agreement), parties to the agreement, data covered, and protection requirements for the data.
- **Connection Type/Data Direction:** IPSec VPN, SSL, Secure File Transfer, API/Incoming, outgoing, or both.
- **Comments:** Any additional comments to describe the data connection.

Table 8. Interconnections and Data Exchange Between EDE Environment Provider and Upstream Entities

ID	Information System Name	Upstream EDE Entity Organization Name	Information Being Transmitted[24]	Data Sharing Agreement in Place	Connection / Data Direction	Comments
1						
2						
3						
4						
5						
6						
7						
8						
9						

[24] Note: A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for the Enhanced Direct Enrollment Entity Information Technology Systems process.

B.3 Additional Functionality or Systems

Instructions: During the annual EDE Agreement Renewal submission of the ISA, Primary EDE Entities must document all approved upstream EDE Entity relationships in Table 9. After the annual EDE Agreement Renewal submission, primary EDE Entities must submit a new Table 9 for each new upstream EDE Entity. If you insert a new Table 9, be sure to update the Table Caption field to ensure the correct, sequential table numbering; update the cross-reference fields for the tables; and update the List of Tables in the front matter. If you copy a table, paste it at an insertion point styled as "Normal" and use the following command: Paste/Paste Special/Formatted Text (RTF) where Track Changes is turned off. **[Delete this instruction.]**

Note: A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems process including performing a Security Impact Analysis (SIA), a Business Impact Analysis (BIA), and potentially updating the 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. **[Delete this instruction.]**

Table 9 contains the following fields:

- **ID:** Unique identifier for the row item to track items between Table 8 and Table 9, as applicable.
- **Information System Name:** IT system environment name for the EDE Environment Provider.
- **Upstream EDE Entity Organization Name:** Document all known or expected upstream entities and/or system name (if applicable).
- **NEW: SSO Implementation:** If an EDE arrangement will involve SSO, the entity must describe the SSO implementation, including, at a minimum, the following information: which users will use the SSO implementation (i.e., consumers, agents, and brokers) and the process to and entity responsible for conducting identity proofing of consumers, agents, and brokers.
- **Additional Functionality/Systems:** For each applicable arrangement, indicate whether the primary EDE Entity's environment integrates with any functionality or systems owned, controlled, managed, or accessed by the upstream EDE Entity that exists outside of the boundaries of the audited, primary EDE Entity's EDE environment. For any such functionality or system, indicate the data transferred between the external environment and the EDE environment (e.g., data regarding data matching issues, special enrollment period verification issues, and enrollment status).
  - In the following sub-bullets, CMS provides several, non-exhaustive examples of potential additional functionality or systems:
    - Example Scenario 1: An upstream EDE Entity collects initial data from a consumer on its system for the purposes of completing an eligibility application or to display health insurance options or QHPs (e.g., plan selection), and then may redirect the consumer and/or their data to the primary EDE Entity for completing the eligibility application or enrollment experience.

- Example Scenario 2: An upstream EDE Entity provides a plan selection and enrollment process separate from the primary EDE Entity's EDE environment.
- Example Scenario 3: An upstream entity provides the agent/broker identity proofing implementation on its own system. Agents and brokers then use the primary EDE Entity's EDE environment to assist consumers.
- Example Scenario 4: An upstream entity retrieves, stores, transfers, or manages consumer data obtained or collected through the primary EDE Entity's EDE environment on the upstream entity's own system (e.g., data stored in a customer relationship management software).
- Example Scenario 5: An upstream entity implements a single sign-on solution with the primary EDE Entity's EDE Environment.

- **REVISED: QHP Display for EDE End-User Experience:** For each arrangement, indicate whether the primary EDE Entity or upstream EDE Entity provides the QHP display for the EDE End-User Experience. If both the primary and upstream EDE Entity provide the QHP display—such as at different parts of the EDE End-User Experience or for different pathways (e.g., agent/broker and consumer), describe the details of the arrangement for displaying QHPs in the End-User Experience for both agents/brokers and consumers.
  - For example, the upstream EDE Entity sends a selected QHP to the primary EDE Entity before a user completes the eligibility application, and the primary EDE Entity provides a post-application QHP shopping experience.
  - Another example, the upstream EDE Entity hosts a pre-application QHP display for agents/brokers and sends the QHP selection to the primary EDE Entity. The primary EDE Entity hosts the QHP display for consumers.
- **Comments:** Any additional comments to describe the data connection.

Table 9. Additional Functionality or Systems

ID	Information System Name	Upstream EDE Entity Organization Name	SSO Implementation[25]	Additional Functionality[26]	QHP Display for EDE End-User Experience[27]	Comments
1						
2						
3						
4						
5						

[25] CMS has added this new field to Table 9. Please review the instructions above to provide an appropriate response to this field.

[26] Note: A primary EDE Entity adding any EDE Entity relationships must also follow the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems process.

[27] CMS has revised the instructions for this field. Please carefully review the instructions above to provide an appropriate response to this field.

B.4 Data Flow/Topological Diagram

Instructions: Describe the flow of data in and out of the Primary EDE Environment and Additional Systems/Functionality system boundaries and insert a data flow/topological diagram. Describe protections implemented at all entry and exit points in the data flow. If necessary, include multiple data flow/topological diagrams.

To insert a figure object, style the insertion point as "Figure" and paste the object as a Picture (Enhanced Metafile) or .png. **[Delete this instruction.]**

Figure 2 represents the data flow in and out of the Primary EDE Environment and Additional Systems/Functionality system boundaries.

Figure 2. Data Flow/Topological Diagram