

DEPARTMENT OF HEALTH & HUMAN SERVICES  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard, Mail Stop N3-12-16  
Baltimore, Maryland 21244-1850



**ASSOCIATE INTERCONNECTION SECURITY AGREEMENT**

**BETWEEN THE**

**CENTERS FOR MEDICARE & MEDICAID SERVICES**

**AND**

**THE [CONNECTING ENTITY]**

**CONNECTING TO CMS DATA SERVICES HUB (HUB)**

**Version 1.0**  
**June 19, 2013**

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

**Instructions for completing this form:**

**IMPORTANT: This page contains instructions. To avoid confusion, it should be deleted prior to either hardcopy or electronic distribution of completed draft or final associate ISA.**

[NOTE: While the blank template is subject to no limitations on use or disclosure from CMS perspective, CMS will treat completed templates as potentially sensitive business information, and will only disclose completed templates as required by law.]

In filling out the form, the Connecting Entity should replace everything inside the brackets “[Connecting Entity]” with the name of, or, if established the first time the full name is written out, the shorthand reference for, the Non-Federal signatory to this agreement.

The information provided in “<< . . . >>” throughout this template provide instruction as to what is to be inputted in that section of the template. Replace these instructions with the requested information. No instructional information should be retained in the final document.

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

**TABLE OF CONTENTS**

1.	PURPOSE.....	4
1.1	RELATIONSHIP TO OTHER AGREEMENT DOCUMENTS AND LEGAL OBLIGATIONS.....	5
1.2	THE CMS ACA ISA MANAGEMENT PROCESS.....	6
2.	[CONNECTING ENTITY] BACKGROUND.....	6
2.1	[CONNECTING ENTITY] INFORMATION SECURITY PROGRAM.....	6
2.2	SECURITY POLICIES.....	7
2.3	ROLES AND RESPONSIBILITIES.....	7
2.3.1	SYSTEM OWNER.....	7
2.3.2	SYSTEM PLANNING.....	7
2.3.3	SYSTEM SECURITY.....	7
2.3.4	CE AUTHORIZED OFFICIAL.....	8
3.	SCOPE.....	8
4.	AUTHORITIES & REFERENCES.....	8
5.	STATEMENT OF REQUIREMENTS.....	10
5.1	[CONNECTING ENTITY] SYSTEM DESCRIPTION.....	10
5.2	GENERAL INFORMATION/DATA DESCRIPTION.....	10
6.	DATA SENSITIVITY AND METHODS OF INTERCONNECTION.....	10
6.1	DATA SENSITIVITY LEVEL.....	10
6.2	CE EXTERNAL CONNECTIONS.....	10
6.3	METHODS OF INTERCONNECTION TO THE HUB.....	11
7.	INFORMATION PROTECTION REQUIREMENTS.....	11
7.1	COMMITMENT TO PROTECT SENSITIVE INFORMATION.....	11
8.	PERSONNEL SECURITY.....	12
8.1	RULES OF BEHAVIOR.....	12
8.2	ACCESS MANAGEMENT.....	12
8.3	TRAINING AND AWARENESS.....	12
8.4	PERSONNEL CHANGES / DE-REGISTRATION.....	13
9.	SECURITY DOCUMENTATION.....	13
10.	PHYSICAL SECURITY.....	14
11.	NETWORK SECURITY.....	14
11.1	NETWORK MANAGEMENT.....	14
11.2	NETWORK DOCUMENTATION.....	14
12.	MEDIA PROTECTION.....	14
13.	INCIDENT PREVENTION, DETECTION, AND RESPONSE.....	15
13.1	INCIDENT HANDLING.....	15
13.2	CE INTERNAL COMMUNICATION AND RESPONSE.....	16
13.3	DISASTERS AND OTHER CONTINGENCIES.....	16
14.	CHANGE MANAGEMENT.....	17
14.1	PERSONNEL CHANGES.....	17

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [\[Connecting Entity\]](#)

14.2 CHANGES TO THE ASSOCIATE ISA .....17

14.3 INTERCONNECTION CHANGES .....17

    14.3.1 NEW INTERCONNECTIONS ..... 17

    14.3.2 MODIFICATIONS TO EXISTING INTERCONNECTIONS ..... 17

    14.3.3 TERMINATION OF INTERCONNECTIONS..... 17

15. ASSOCIATE ISA MAINTENANCE.....19

16. ATTESTATION AND SIGNATURES.....19

## **1. PURPOSE**

This Associate ISA between the [Connecting Entity] and the Centers for Medicare & Medicaid Services (CMS), combined with the CMS Master Interconnection Security Agreement (ISA) dated June 19, 2013 version 1.0 which is attached, establishes approval for system-to-system data exchanges between the undersigned parties through a connection to the CMS Data Services Hub (the Hub). Such connectivity is made available in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148) as amended by the Health Care and Education Reconciliation Act (Public Law 111-152) (which are collectively as the Affordable Care Act (ACA)).

45 C.F.R. §155.260(b) provides authority for Exchanges to make disclosures to non-exchange entities for the purpose of performing Exchange minimum functions (45 C.F.R. §155.200) pursuant to agreements or contracts that bind such non-Exchange entity to as stringent or more stringent privacy and security standards as articulated in §155.260.

In executing this Associate ISA, the undersigned establish the security controls that will be imposed on their system-to-system access to data through the Hub. The non-federal signatory is hereafter referred to as the “Connecting Entity” or (CE).

To this end, each security control should be captured by the CE in their ACA System Security Plan (SSP) workbook in accordance with the Minimum Acceptable Risk Standards for Exchanges (MARS-E) version 1.0 which can be found in at: <http://cciio.cms.gov/resources/regulations/index.html>. The completed SSP workbook will outline the Connecting Entity’s security control requirements, the manner in which the CE intends to implement those requirements, and any compensating controls that may be required for the systems to remain in full compliance with MARS-E and other requirements laid out in this agreement and any other applicable laws.

## **1.1 RELATIONSHIP TO OTHER AGREEMENT DOCUMENTS AND LEGAL OBLIGATIONS**

Each CE that desires to send or receive Personally Identifiable Information (PII)<sup>1</sup> through the Hub must also complete relevant privacy artifacts (Privacy Impact Assessment (PIA)) and execute the relevant privacy and security artifacts which encompasses both the legal agreements (i.e., computer matching agreements, information exchange agreements, and interconnection security agreements) as well as the operational deliverables (i.e., privacy impact assessments, system security plans, and IRS ACA safeguard procedures reports as defined in the Privacy and Security Timelines and Artifacts For Health Insurance Marketplaces and Partner Organizations<sup>2</sup> document version 1.0 dated April 2013 . These agreements will describe what PII the CE may access through their system-to-system connection to the Hub, and whether and how PII that was obtained through the Hub may be maintained, used, and re-disclosed. Such descriptions will include the privacy standards for the protection of PII obtained through the Hub. No PII may be exchanged until all relevant documents are fully executed.

In signing this agreement the signatories also acknowledge that they must meet all applicable laws that govern their data access, maintenance, use and disclosure. This agreement does not obviate any obligations that are otherwise required by such laws. For example, Internal Revenue Code (IRC) 26 U.S.C. §6103 (p)(4) and Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, available at <http://www.irs.gov> applies if an Administering Entity IT system receives Federal Tax Information. Therefore, Connecting Entities must develop their IT systems to comply with these more stringent standards when applicable.

The Associate ISA demonstrates how the Connecting Entity will meet the requirements laid out in the Master ISA.

---

<sup>1</sup> For purposes of this document, PII is defined in the same manner as OMB defined it in Memorandum M-07-16, which provides “refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”

<sup>2</sup> Refer to *Privacy and Security Timelines and Artifacts For Health Insurance Marketplaces and Partner Organizations*.

## **1.2 THE CMS ACA ISA MANAGEMENT PROCESS**

Derived from the NIST SP 800-47 guidance, the CMS ISA management process involves the following three steps:

- **Step 1: Develop Implementation Plan**

This involves identifying the technical and security requirements governing the interconnection. The Master ISA and Associate ISA template are the outputs of this process.

- **Step 2: Execute Implementation Plan**

This involves engineering, implementing, and testing of the connection, as well as the documentation of the interconnection security controls and procedures. Documentation of the implementation details is included in an SSP.

- **Step 3: Activate Interconnection**

The authorized official of the Connecting Entity submits to CMS, by way of this Associate ISA, the request for Approval to Connect (ATC) to the Hub, based on attestation in Section 16 of this document that the system meets all the requirements stated in the Associate ISA. The request for ATC, via the Associate ISA, needs to be accompanied by the relevant supporting documentation as indicated in Section 3.1 (Artifacts Nuisance) paragraph titled Critical Path for an Authority to Connect (ATC) to the CMS Federal Data Services Hub. The CMS Chief Information Officer, based on evaluation of risk, either grants by signing the Associate ISA or denies the request for ATC in writing.

No personally identifiable data will pass through the network prior to an ATC.

## **2. [CONNECTING ENTITY] BACKGROUND**

<<Describe the background and mission of the Connecting Entity as it related to their need for access to network connectivity to the Hub>>

### **2.1 [CONNECTING ENTITY] INFORMATION SECURITY PROGRAM**

<<Provide a description about the IT Security Program of the Connecting Entity, as it relates to their need for access to network connectivity to the Hub, that helps the organization accomplish its mission by ensuring the confidentiality, integrity, and availability of the CE information resources. For example, the CE has developed policies and procedures to ensure adequate security of their information systems to comply with Federal and state laws/regulations. The CE monitors the security of their systems/networks 24 hours a day, seven days a week (24 x 7), through management, operational, and technical processes. >>

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

**2.2 SECURITY POLICIES**

<<Provide the titles and dates of any formal security policies, guidelines, or standard operating procedures the CE has for their IT security program. >>

**2.3 ROLES AND RESPONSIBILITIES**

<< The Connecting Entity agrees to provide contact information for business owner and technical leads for their respective system/network to support the management and operation of the interconnection. If more than one point of contact exists, please specify by indicating as primary, secondary or alternate 1 or alternate 2, etc.

Also, provide a brief description of each role and associated responsibilities for implementing information technology and information security (IS) policies, procedures, and tools that support confidentiality, integrity, and availability (CIA). >>

**2.3.1 SYSTEM OWNER**

<<The following individual is identified as the system owner for this system or application. Provide a description of the individual roles and responsibilities :>>

<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	

**2.3.2 SYSTEM PLANNING**

<<The following are the points of contact that have in-depth knowledge of the Connecting Entity’s system. Provide a description of the individuals’ roles and responsibilities :>>

<b>Primary Point-of-Contact</b>			
<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	
<b>Secondary Point-of-Contact</b>			
<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	

**2.3.3 SYSTEM SECURITY**

<<The following individuals are identified as the Information System Security Officers (ISSOs) for the Connecting Entity’s system. Provide a description of the individuals’ roles and responsibilities :>>

<b>Primary Point-of-Contact</b>			
<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	
<b>Secondary Point-of-Contact</b>			

## CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Associate ISA between CMS and the [\[Connecting Entity\]](#)

<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	

### 2.3.4 CE AUTHORIZED OFFICIAL

*<<The following individual is a legally authorized representative of the Connecting Entity and able to enter the CE into this agreement with CMS. Provide a description of the individual roles and responsibilities :>>*

<b>Name:</b>		<b>Address:</b>	
<b>Title:</b>		<b>Phone Number:</b>	
<b>Department:</b>		<b>Email Address:</b>	

## 3. SCOPE

The scope of this Associate ISA includes the following:

- The following entities are eligible to become connecting entities:
  - Administering Entities: Exchanges, whether Federal or State, State Medicaid agencies, State Children’s Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program (BHP).
  - State-based entities that provide data routing service for state AE systems. For this situation, the Associate ISA will describe (in Section 6) the connection and data flows between the service provider and entities being served.
  - Service providers in support of a state participating in the State Partnership Exchange model. These are agents of the state exchange.
  - Service providers in support of the Federally Facilitated Exchange (FFE). These are agents of the FFE.
- Employees/Contractors managing, engineering, accessing, or utilizing the CE system.

## 4. AUTHORITIES & REFERENCES

The authorities for this Associate ISA are based upon, but are not limited to, the following:

- 18 U.S.C. §641, Criminal Code: Public Money, Property or Records
- Privacy Act of 1974, 5 U.S.C. § 552a. System of Records Notice citation: “Health Insurance Exchanges Program” 78 Federal Register 8538, February 6, 2013

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

### Associate ISA between CMS and the [Connecting Entity]

- The Patient Protection and Affordable Care Act of 2010, P.L. 111-148 as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111-152). Together, these laws are referred to as “the Affordable Care Act” (ACA). Sections 1411 and 1413 of the ACA provide authority to make disclosures to the Administering Entities.
- 45 C.F.R. §155.260(b) provides authority for Exchanges to make disclosures to non-exchange entities for the purpose of performing Exchange minimum functions (45 C.F.R. §155.200) pursuant to agreements or contracts that bind such non-Exchange entities to as stringent or more stringent privacy and security standards as articulated in §155.260. Section 1943(b) of the Social Security Act (as added by section 2201 of the ACA) requires Medicaid and CHIP agencies utilize the same streamlined enrollment system and secure electronic interface established under Section 1413 of the ACA to verify information, including citizenship and satisfactory immigration status, needed to make an Eligibility Determination and facilitate a streamlined eligibility and enrollment system among all insurance affordability programs. 45 C.F.R §§ 155.302 and 155.305 require that a Marketplace determine or assess individual eligibility for Medicaid/CHIP in certain circumstances and ensure that those individuals are enrolled in Medicaid/CHIP coverage

The references for this Associate ISA are based upon, but are not limited to, the following:

- The Health and Human Services Final Rule on Exchange Establishment also requires that all Federal Tax Information (FTI)<sup>3</sup>, as defined in section 6103(b)(2) of the Internal Revenue Code (IRC), be kept confidential and disclosed, used, and maintained only in accordance with section 6103(p)(4) of the IRC as a condition of receipt of FTI and the Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*
- *Minimum Acceptable Risk Standards for Exchanges* (MARS-E) Document Suite version 1.0, August 1, 2012 which consists of the following seven documents:
  - *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement*
  - *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement*
  - *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*
  - *ACA System Security Plan Procedures*
  - *ACA System Security Plan Template*

---

<sup>3</sup> FTI generally, Federal tax returns and return information are confidential, as required by IRC §6103.

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

- *ACA System Security Plan Workbook*
- *IRS ACA Safeguard Procedures Report Template*

### **5. STATEMENT OF REQUIREMENTS**

#### **5.1 [CONNECTING ENTITY] SYSTEM DESCRIPTION**

<< Provide a functional description of the system connecting to Data Services Hub. >>

#### **5.2 GENERAL INFORMATION/DATA DESCRIPTION**

<<At a general level, provide a description of the business requirements for the interconnection between the Connecting Entity and Data Services Hub. Include the type of information and data that will be made available, exchanged, or passed one-way only, by the interconnection of the two systems/networks. For example, verification of coverage eligibility, data for paying insurers and data for use in portals for consumers. >>

### **6. DATA SENSITIVITY AND METHODS OF INTERCONNECTION**

The [Connecting Entity] avows to protect Hub-acquired data in order to maintain confidentiality, integrity, and availability of the Hub data and CMS' information systems. In order to receive approval for the CE's networks to connect to the CMS Data Services Hub, adequate security controls must be fully implemented and documented in an SSP in accordance with MARS-E.

#### **6.1 DATA SENSITIVITY LEVEL**

The overall sensitivity level of data or information that will be made available, exchanged, or passed one way only across the interconnection will be designated as **MODERATE** as determined by Federal Information Processing Standards (FIPS) Publication 199.

<< Provide a description about the information handled by the system and the overall system security level as **LOW** or **MODERATE**. Refer to the *CMS Information Security Levels* document on <http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf>. >>

#### **6.2 CE EXTERNAL CONNECTIONS**

<< Identify connections exclusive of any connection to the Hub and provide a description of the business relationship between the CE and interconnected external systems, nature of data communication and services provided. >>

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

### **6.3 METHODS OF INTERCONNECTION TO THE HUB**

<<Provide a description about the nature of the data communication services (e.g. E-mail, SFTP, data base query, file query, general computational services, etc.) offered over the interconnection. Include specific protocols, ports, and services that are needed to support this interconnection. >>

#### **Topological Diagram (end-to-end)**

<< Include a network topology that depicts the interconnectivity between Data Services Hub and the Connecting Entity 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, as well as the security controls deployed for each method of connection as cited in the SSP. >>

## **7. INFORMATION PROTECTION REQUIREMENTS**

### **Connecting Entity avows that it will:**

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

### **7.1 COMMITMENT TO PROTECT SENSITIVE INFORMATION**

#### **In executing this agreement, Connecting Entity avows that it will:**

- Not release, publish, nor disclose Hub and Hub-derived PII to unauthorized individuals.
- Protect such information in accordance with applicable law and the provisions of this Associate ISA and the Master ISA. Ensure that its officers, employees and contractors who have access to this data will sign an appropriate Rules of Behavior or non-disclosure agreement.
- Not store PII obtained through or derived from the Hub outside the United States, its territories and possessions.
- Ensure that its contractors shall comply with the security requirements set forth in this agreement, and the organization's specific information security policies, standards, and procedures.
- The Health and Human Services Final Rule on Exchange Establishment also requires system processing Federal Tax Information (FTI), as defined in section 6103(b)(2) of the Internal Revenue Code (IRC), be kept confidential and disclosed, used, and maintained only in accordance with section 6103(p)(4) of the IRCs a condition of receipt of FTI. FTI may not be accessed by agency employees, agents, representatives or contractors located “offshore”, outside of the United States or its territories. Further, FTI may not be received, stored, processed or disposed via information technology systems located off-shore.

## **8. PERSONNEL SECURITY**

<< Provide the policies and procedures that address personnel security controls for employees and contractors. Explain whether users are subject to an appropriate background check prior to their being given access to the Connecting Entity systems and networks that connect to the Hub. >>

### **8.1 RULES OF BEHAVIOR**

Rules of Behavior describe information system user responsibilities and expected behavior with regard to information and information system usage.

#### **Connecting Entity avows that it will:**

- Ensure that all users with access to the Connecting Entity's and its connection with the Hub adhere to the privacy and security agreements executed by the CE (as defined in the Privacy and Security Timelines and Artifacts For Health Insurance Marketplaces and Partner Organizations document in Section 3.1 (Artifacts Nuisance) paragraph titled Critical Path for an Authority to Connect (ATC) to the CMS Federal Data Services Hub) and where not in conflict with their organization's Rules of Behavior.
- Ensure the organization's Rules of Behavior are adequate compared to HHS Rules of Behavior: [http://www.hhs.gov/ocio/policy/hhs-ocio-2010-0002.001s\\_hhs\\_rules\\_of\\_behavior.html](http://www.hhs.gov/ocio/policy/hhs-ocio-2010-0002.001s_hhs_rules_of_behavior.html).

### **8.2 ACCESS MANAGEMENT**

<< Provide the policies and procedures that address access management for employees and contractor. This refers to SSP on Access Controls (AC). >>

#### **Connecting Entity avows that it will:**

Enforce the following access control principles:

- Least Privilege: Only authorizing access to the minimal amount of resources required for a function.
- Separation of Duties: Utilize a basic system of controls that prevents and/or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions, and custody of assets to separate individuals.
- Role-Based Security: individuals derive their access rights from the role they are performing.

### **8.3 TRAINING AND AWARENESS**

<<Provide the details of any security awareness, training requirements, and the assignment of responsibility for conducting it throughout the life cycle of the interconnected system. >>

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

### **Connecting Entity avows that it will:**

- Prior to granting employees and contractors employees with access to the connecting entity's network connections to the Hub, or PII obtained through the Hub, ensure that these individuals complete appropriate information security and awareness training and then annually thereafter.
- Prior to granting an employee or contractor access to Federal tax information (FTI), and annually thereafter, ensure that each individual employee or contractor employee completes FTI training that covers the penalties for unauthorized disclosure and access to FTI and acknowledge receipt of the training and sign a confidentiality statement See IRS Publication 1075 requirements, Section 6.2 at <http://www.irs.gov/pub/irs-pdf/p1075.pdf> .

## **8.4 PERSONNEL CHANGES / DE-REGISTRATION**

### **Connecting Entity avows that it will:**

Notify CMS of any personnel changes involving their points of contact identified in their Associate ISA section 2.3 (Roles and Responsibilities), including the separation of their system owners or technical leads by contacting the CMS IT Service Desk via e-mail to [CMS\\_IT\\_Service\\_Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov).

## **9. SECURITY DOCUMENTATION**

### **Connecting Entity avows that it will:**

- Ensure information security consideration is planned, managed, and documented using a system development lifecycle methodology such as the one outlined in the *Catalog of Minimum Acceptable Risk Controls for Exchanges- Exchange Reference Architecture Supplement* dated August 1, 2012 version 1.0, section System and Services Acquisition (SA) - Management.
- Maintain a current SSP on the Connecting Entity's network. The SSP and relevant artifacts shall be reviewed annually and updated whenever there is a change that impacts the security of the system. Whenever a change has occurred, a security impact assessment should be conducted pursuant to MARS-E requirements to determine whether there are impacts to the security posture of the system. Any changes impacting the security of the system should be reflected in the SSP.
- Upon request, make accessible to CMS all information security program documents as cited in the CE's SSP.

## **10. PHYSICAL SECURITY**

The Connecting Entity avows that it will implement and document the physical security measures listed in the Master ISA.

## **11. NETWORK SECURITY**

### **11.1 NETWORK MANAGEMENT**

**Connecting Entity avows that it will:**

- Ensure the security of the information being exchanged or transmitted on this two-way connection is protected through the use of FIPS 140-2 validated encryption algorithms.
- Ensure that the CE connection is located within controlled access facilities, guarded 24 hours a day, or use a two-factor authentication for entry.
- Ensure that individual users will only have access to the ACA data through secure access control mechanisms as spelled out in MARS-E.
- Ensure that each of the modes of interconnection is isolated from other customers and business processes and protected via FIPS 140-2 validated encryption.
- Ensure that connection sessions are authenticated using an MARS-E compliant authentication mechanism. Dual certificate exchange is preferred.
- Protect data exchanged over this interconnection in accordance with the Privacy Act, 5 U.S.C. §552a.

### **11.2 NETWORK DOCUMENTATION**

**Connecting Entity avows that it will:**

- Maintain adequate documentation that describes the design and implementation details of their interconnected system boundaries (i.e., Data Services Hub, Exchange), and security controls employed within the information system.
- Upon CMS request, make such documentation available to CMS for review.

## **12. MEDIA PROTECTION**

The Connecting Entity avows that it will implement and document the Media Protection provisions listed in the CMS Master ISA.

## **13. INCIDENT PREVENTION, DETECTION, AND RESPONSE**

Refer to the Master ISA for definitions of the terms “incident” and “breach.” The use of the Data Services Hub constitutes consent to CMS monitoring and auditing of usage at any time.

The Connecting Entity avows that it will maintain audit trail records that will be sufficient in detail according to MARS-E to facilitate the reconstruction of events if compromise or malfunction is confirmed or suspected. Audit records shall be reviewed as specified in each Connecting Entity’s SSP.

### **13.1 INCIDENT HANDLING**

Each party to the agreement reserves the right to terminate interconnection to mitigate or avoid any immediate or recurring risks to the security their system.

#### **Connecting Entity avows that it will:**

- Have documented organizational policies and procedures that address how to do the following:
  - Handle and report incidents in accordance with the organization’s documented incident handling and breach notification procedures within their Incident Response Plan. Connecting Entities’ procedures should address how they will:
    - Identify incidents
    - Determine if personally identifiable information is involved in incidents
    - Report suspected or confirmed incidents
    - Identify and convene a core response group within the Connecting Entity who will determine the risk level of incidents and determine risk-based responses to incidents
    - Determine whether breach notification is required, and, if so, identify appropriate breach notification methods, timing, source, and contents from among different options
    - Disclose information about individuals (whose information may have been compromised, misused, or changed without proper authorization and the persons who disclosed the PII improperly) to authorized federal, state, or local law enforcement investigators in connection with efforts to investigate and mitigate the consequences of any security incidents
  - CEs shall report suspected or confirmed security incidents within one hour of discovery to their designated CCIIO State Officer who will then notify the affected Federal agency data sources, i.e., Internal Revenue Service, Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management and Veterans Health Administration. Additionally,

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

### Associate ISA between CMS and the [Connecting Entity]

CEs shall contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards within 24 hours of discovery of any potential breach, loss, or misuse of FTI. Contact information is contained in Section 10.1, IRS Publication 1075, <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

## **13.2 CE INTERNAL COMMUNICATION AND RESPONSE**

### **Connecting Entity avows that it will:**

- Require all staff and contractors to report security incidents directly to the appropriate individuals as identified in the Connecting Entity's Incident Responses Plan within one hour on all interconnected automated information systems covered by this interconnection security agreement.
- Block inbound and outbound access for any automated information system within the scope of this Associate ISA and the Master ISA that are the source of unauthorized access attempts, or the subject of any security events, until the risk is analyzed and remediated.
- Ensure their Incident Response Plan as required by MARS-E contains up-to-date contact information for personnel handling interconnection security-related incidents.

## **13.3 DISASTERS AND OTHER CONTINGENCIES**

Maintaining continuity of service for the users of ACA systems is of utmost importance to the mission.

### **Connecting Entity avows that it will:**

- Maintain an up-to-date system contingency plan.
- Ensure that its contingency plan addresses, for each mode of connectivity with partner organizations and with CMS, the following:
  - Methods for maintaining essential business functions in the event of an information system disruption, compromise, or failure (on either side).
  - Procedures for eventual, full-service resumption and information system recovery.
  - Emergency alert and notification procedures and points of contact.
- Ensure the contingency plan and other related plans including the incident response plan pertaining to CMS system-to-system connectivity through the Hub and the protection of PII obtained through the Hub are tested annually.
- Assign personnel to coordinate with connecting partner organizations' joint activities in contingency planning, training, and testing exercises.

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

### Associate ISA between CMS and the [Connecting Entity]

- Make the necessary notifications as laid out in their information system contingency plan(s) in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected networks.

## **14. CHANGE MANAGEMENT**

The Connecting Entity avows that it will implement and document the change management measures listed in the Master ISA.

### **14.1 PERSONNEL CHANGES**

As described in Section 8.4, if any personnel changes occur involving the POCs listed in this Associate ISA, the terms of this Associate ISA shall remain in full force and effect, unless formally modified or terminated by both parties.

### **14.2 CHANGES TO THE ASSOCIATE ISA**

Any changes to this Associate ISA must be mutually agreed upon and approved in writing by the signatories of this document or their successors.

### **14.3 INTERCONNECTION CHANGES**

#### **14.3.1 NEW INTERCONNECTIONS**

##### **Connecting Entity avows that it will:**

Notify CMS when new interconnections impact the security posture unless expressly agreed upon in a modification to the relevant Associate ISA and signed by both parties.

This agreement allows the CE to connect test environments as required in the testing process provided they do not contain production data or violate the other terms of the ISA.

#### **14.3.2 MODIFICATIONS TO EXISTING INTERCONNECTIONS**

The Connecting Entity ensures the existence of an organizational Change Control Board (CCB) that reviews and approves changes to its respective application and infrastructure system, such as upgrading software or adding services. The CCB review process shall include an ISA impact assessment to ensure the ISA Points of Contact are involved as necessary. Documentation of the reviews should be maintained for 3 years and made available to CMS and/or its designee upon request.

#### **14.3.3 TERMINATION OF INTERCONNECTIONS**

Impacted parties shall be notified prior to the termination of an interconnection (unless in emergency situations) to safeguard the network, system, or data.

## **CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [\[Connecting Entity\]](#)

### **Emergency Disconnection**

#### **Disconnection by CMS:**

If there is a suspected security incident or event that may warrant an emergency disconnect of CMS' system-to-system connection with CE, CMS will notify CE's <<insert Points of Contact, number(s) and email addresses>>. The CMS' internal security components will then address the incident or event following internal procedures and processes and will involve the appropriate CE components and external agencies. Upon resolution of the incident, an "after action report" will be presented to CE senior management, and, if at that time it is deemed "safe" to restore the connection, both sides will follow restoration and organizational change management procedures.

#### **When the CE needs to make a disconnection, CE avows to use the following process:**

If there is suspected security incident or event that may warrant an emergency disconnect of CE's system-to-system connection with CMS, the CE will notify the CMS IT Service Desk by calling 410-786-2580 or 1-800-562-1963, or via e-mail to [CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov). The Connecting Entity will then follow Incident Response Procedures currently based on their Computer Security Incident Response Program. Upon resolution of the incident, an "after action report" will be presented to CMS Information System Security Officer and, if at that time it is deemed "safe" to restore the connection, both sides will follow restoration and organizational change management procedures.

### **Restoration of Interconnection**

Both organizations may choose to restore the network interconnection after it has been terminated. The decision to restore the interconnection should be based on the cause and duration of the disconnection. For example, if the interconnection was terminated because of an attack, intrusion, or other contingency, both parties should implement appropriate countermeasures to prevent a recurrence of the problem. If necessary, they also should modify the Associate ISA and any other necessary agreements to address issues requiring attention. Alternately, if the interconnection has been terminated for more than 90 days, each party should perform a risk assessment on its respective system and re-examine all relevant planning and implementation requirements, including developing a new ISA and relevant agreements.

### **Planned Disconnection**

A planned disconnect should be coordinated with the CE internal business liaison. Said liaison will then notify the appropriate CMS components. Notification of the planned disconnection is given sixty (60) business days before the disconnection takes place.

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [Connecting Entity]

**15. ASSOCIATE ISA MAINTENANCE**

Proper management of the network interconnection ensures the confidentiality, integrity, and availability of the data is maintained. After interconnections are established between CMS and the CE, **the CE avows that it will:**

- Internally monitor and control its system interconnections on an ongoing basis. This should include configuration control and audit trail analysis.
- Conduct reviews of the Associate ISA, including associated security artifacts, on a yearly basis.
- Re-sign the Associate ISA every three (3) years or whenever both parties agree that a significant change has occurred to any of the interconnected systems.

**16. ATTESTATION AND SIGNATURES**

We agree to the terms and conditions of the Master ISA and this Associate ISA.

CMS and Connecting Entity agree to work together to ensure the joint security of the connected networks and the data they store, process, and transmit, as specified in the above-referenced Master ISA and this Associate ISA. By signing below, the Connecting Entity certifies that all of the assertions above and that its respective system is designed, managed, and operated in compliance with Minimum Acceptable Risk Standards for Exchanges (MARS-E).

The CMS CIO signature provides [Connecting Entity] the Authority to Connect (ATC) to the Data Services Hub.

**Connecting Entity**

Authorized Official of CE	Signature	Date

(I attest that I am a legally authorized representative of the CE and able to enter the CE into a binding contract.)

**Where the Connecting Entity is an agent of an Administering Entity**

Authorized Official of AE	Signature	Date



## **APPENDIX A – ACRONYM LIST**

AC	Access Control
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
ATC	Approval to Connect
BHP	Basic Health Program
BO	Business Owner
CALT	Collaborative Application Lifecycle Tool
CCB	Change Control Board
CE	Connecting Entity
CHIP	Children’s Health Insurance Program
CIA	Confidentially, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Computer Matching Agreement
CMCS	Center for Medicaid and CHIP Services
CMS	Centers for Medicare & Medicaid Services
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HTTP	Hypertext Transfer Protocol Secure
HTTPS	Hypertext Transfer Protocol
HUB	Data Services Hub
IEA	Information Exchange Agreement
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information Security
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	Information Technology
MARS-E	Minimum Acceptable Risk Standards for Exchanges
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Point of Contact
SFTP	Secure File Transfer Protocol

**CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING**

Associate ISA between CMS and the [\[Connecting Entity\]](#)

SMTP	Simple Mail Transfer Protocol
SP	Special Publication
SSP	System Security Plan
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Readiness Team