Computer Matching Agreement (CMA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The CMA documents the terms and conditions for Computer Matching, which involves the computerized comparison of two or more automated systems of records, or of a system of records with non-Federal records.	• Authorized Federal Approving Official (ex. Recipient Agency)	• CMS Program Official • CMS Approving Official (Privacy) • HHS Data Integrity Board (DIB) Chairperson	Initial CMA duration is 18 months. After 18 months, the CMA may be extended once for an additional 12 months. After the extension time period, the CMA renewal restarts the initial 18 month cycle.

Guidance: The CMA is required when the Computer Matching and Privacy Protection Act (CMPPA) applies. The records must exist in automated/electronic form or be converted to automated form to perform the match. The computerized matching of records can be used to verify the eligibility of or continuing compliance with statutory or regulatory requirements by, applications for, recipients or beneficiaries of, participants in, or providers of services with respect to cash in kind assistance or payments under Federal benefit programs. In addition, the CMA can support the recouping of payments or delinquent debts under such Federal benefit programs. The state cannot initiate a CMA. Additional information on CMA can be found here.

Data Use Agreement (DUA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The DUA tracks disclosures of Personally Identifiable Information (PII) and/or Protected Health Information (PHI) to third parties, to ensure that any transaction of data is compliant with the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.	• **Authorized Federal Approving Official (ex. CMS Contracting Officer's Representative (COR))**	• **CMS Program Official, (e.g. COR, Privacy Board Chair)**	**Initial 1-year duration, then may be renewed as needed.**

Guidance: The DUA can involve third party entities, such as oversight agencies, Federal agencies, state agencies, research institution, and The DUA template and additional guidance can be found here.

Inter-Agency Agreement (IAA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The IAA is established when CMS agrees to provide materials, supplies, equipment, work or services that another Federal agency or department needs to accomplish its mission. The source agency is reimbursed for the specified work or provisions.	• **Authorized Federal Approving Official (ex. COR)**	• **CMS Program Official / COR** • **CMS Approving Official/Business Owner** • **CMS Office of Acquisitions and Grant Management**	**1-year duration.**

Guidance: The IAA is used when one Federal agency/department outside of the HHS operating division structure is in a position to provide materials, supplies, equipment, work or services that another Federal agency or department needs to accomplish its mission. In contrast, an Intra-Agency Agreements (IA) is a similar agreement used when one of the HHS operating divisions are in a position to provide materials, supplies, equipment, work or services that another HHS Component needs to accomplish its mission. An IAA that involves the use or disclosure of PII and PHI require an underlying agreement, such as an Information Exchange Agreement (IEA) or Memorandum of Understanding/Agreement (MOU/A).

Information Exchange Agreements (IEA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The IEA documents the terms and conditions for authorized disclosures of CMS data or the receipt of data from another federal or state agency. CMS is responsible for providing the templates for signature for an IEA, when disclosing data. The IEA specifies the Terms, Conditions, and Safeguards for sharing PII/PHI.	• **Authorized Federal Approving Official/Business Owner (ex. Recipient Agency)**	• **CMS Program Official** • **CMS Senior Official for Privacy**	**5-year duration or as specified in the documentation.**

Guidance: The IEA is required when CMS exchanges PII/PHI with another Federal or State agency, or when data is exchanged between a Federal agency, or in some cases, a non-Federal agency. All IEAs include a Data Use Agreement as an attachment (Form: CMS-R-0235). Inter-Agency Agreement (IAA) or Reimbursable Agreement (RA) may be accompanied by an IEA when it involves the disclosure of PII/PHI. The IEA template can be found here.

Interconnection Security Agreement (ISA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The ISA specifies the technical and security requirements for establishing, operating, maintaining and terminating interconnections between IT systems that are owned and operated by different organizations and that are authorized by different Authorizing Officials.	• **Authorized third party equivalent Project Manager, Chief Information Security Office (CISO), Information System Security Officer (ISSO), and Business Owner.**	• **CMS CISO**	**As specified in the agreement. To be reviewed on an annual basis or reauthorized in the event a system is modified via a major change which triggers re-accreditation.**

Guidance: The ISA is the governance document where security risk exposures created by the interconnection of one IT system to another IT system owned by an external entity is identified and defines each parties' responsibilities to manage those risks. The ISA ensures the adequate security of CMS information being accessed and provides that all network access satisfies the mission requirements of both CMS and Non-CMS Organization. The ISA template can be found here. The ISA is based on the NIST SP 800-47 – Security Guide for Interconnecting Information Technology Systems.

Memorandum of Agreement (MOA) / Memorandum of Understanding (MOU)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The MOA/U outlines the terms and conditions regarding the development, management, operation, and security of an interconnection between organizational entities for the purpose of establishing a joint project in which they each contribute their own resources and the scope of work is very broad and generally not specific to any one project and there is no exchange of funds between the partners.	• **Authorized Federal Approving Official/Business Owner (ex. Agency)**	• **Office/Program Director level or higher, from both parties involved.**	**ATO Accreditation period with the potential of extension or as specified otherwise.**

Guidance: The MOU/MOA may provide for trailing Inter/Intra-agency Agreements (IA) that will establish a reimbursable agreement between the partners of a MOU/MOA, where it is determined that funds need to be exchanged. Federal policy requires agencies to develop Interconnection Security Agreements (ISA) or MOUs for system interconnections. CMS has established a standard that an Interconnection Security Agreement (ISA) is employed when the system interconnection is between separate, but secure networks while MOUs are used for interconnections within the same secure network. The MOU template can be found here. The MOU is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47 – Security Guide for Interconnecting Information Technology Systems.

Service Level Agreement (SLA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The SLA specifies relevant service/operational/organization level agreement details between a service provider and CMS.	• **Service Provider, including program manager or equivalent.**	• **Service Provider, including program manager or equivalent.** • **CMS contract management staff (e.g. COR)**	**As specified in the contract, and revised upon contract or service provider modification.**

Guidance: The SLA can include information about existing written commitments to provide a particular level of service (e.g. availability percentage, maximum allowable downtime, guaranteed bandwidth provision). This may include pre-established external engagement contract support that can assist and augment the organization's recovery team in the event of a major cyber event. Additional information regarding an SLA can be found in NIST SP 800-184 – Guide for Cybersecurity Event Recovery*.*

Trading Partner Agreement (TPA)

Purpose	Initiating Party	Approval Authority	Renewal Timeframe
The TPA documents an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between a third party and CMS to the agreement per the Health Insurance Portability and Accountability Act of 1996 (HIPAA).	• **Healthcare Provider** • **Qualified Health Plan Issuers** • **CMS** • **Clearinghouse** • **Healthcare entity (varies)**	• **Healthcare Provider** • **Qualified Health Plan Issuers** • **CMS** • **Clearinghouse** • **Healthcare entity (varies)**	**As specified in the contract, and will automatically renew for successive periods**

Guidance: The trading partner agreement can specify various technical requirements for communications protocols, such as how the transactions are to be addressed, what character set must be used, whether receipt will be acknowledged, and more. The HIPAA transaction rule does not require a trading partner agreement, but if one is used, the rule specifies what may not be included in such an agreement. Specifically, the trading partner agreement cannot: change any definition, data condition, or use of a data element, add any data elements or segments to the maximum defined data set, require use of any codes or data elements that are marked "not used" or not in the implementation guide, or change the meaning or intent of the standard's implementation specification.

Appendix A: Additional Agreement Guidance

- **Computer Matching Agreement (CMA):**
  - Describes the terms and conditions when computer matching is employed to conduct many government functions, including establishing or verifying eligibility for Federal benefit programs, or identifying payments/debts owed to government agencies.
- **Data Use Agreement (DUA):**
  - Describes an agreement that establishes the terms and conditions for the disclosure of CMS data to authorized data requesters.
- **Interagency Agreement (IAA):**
  - Describes a financial reimbursement agreement to provide materials, supplies, equipment, work or services that another Federal agency needs to accomplish its mission.
- **Information Exchange Agreement (IEA):**
  - Describes a legal agreement involving the authorized disclosure of CMS data or the receipt of data from another federal or state agency.
- **Interconnection Security Agreement (ISA):**
  - Describes technical and security requirements for secure connections and can ensure data is encrypted while in transit between two information technology (IT) systems (not on the same network).
- **Memorandum of Understanding (MOU):**
  - Describes an understanding or establishes the terms and conditions between two parties to work together to accomplish an objective. An MOU is not legally binding (unless specified), and does not involve the transfer of funds.
- **Memorandum of Agreement (MOA):**
  - Describes a cooperative relationship between two parties to work together on a project or to meet an agreed upon objective. An MOA serves as a legal document and describes the terms and details of the partnership agreement.
- **Service Level Agreement (SLA):**
  - Describes the performance expectations of a vendor in a service contract with CMS. The SLA may or may not be legally binding.
- **Trading Partner Agreement (TPA)**
  - Describes a relationship between CMS and an external healthcare entity(s) to share data and identify the key data sets of interest, standards needed, and other contractual requirements.