Centers for Medicare & Medicaid Services

NIST SP 800-53 Appendix J Privacy Controls

Security Center of Excellence (SCOE)

March 20, 2014

Privacy Control Families
(# of controls in each)

2 - Authority and Purpose (AP)
8 - Accountability, Audit, and Risk Management (AR)
5 - Data Quality and Integrity (DI)
6 - Data Minimization and Retention (DM)
6 - Individual Participation and Redress (IP)
2 - Security (SE)
5 - Transparency (TR)
2 - Use Limitation (UL)

36 total controls

Inherited Controls
TR-2(1) and TR-3

TR-2(1) - Public Website Publication – Enhancement
The organization publishes System of Record Notices (SORN) on its public website.

TR-3 – Dissemination of Privacy Program Information
The organization:
a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Official for Privacy (SOP)/Privacy Officer (PO); and
b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

(compliance description)
The CMS SOP will post them to the CMS.gov website.

Inherited Controls
DI-2(1)

DI-2(1) - Publish Agreements on Website – Enhancement

The organization publishes Computer Matching Agreements (CMA) on its public website.

(compliance description)

The CMS SOP will submit to the DHHS Data Integrity Board (DIB) all CMS CMAs for approval and then post them to the CMS.gov website.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid Controls – stock language

(compliance description)

These are a hybrid controls. In order to inherit this control, individual program officials and IT system managers must be organizationally bound to and following the controlling CMS content listed in the referenced Policy for Information Security and Privacy Program (PISP-P) and Risk Management Handbook (RMH) for Privacy.

Hybrid
AR-1

AR-1 – Governance and Privacy Program

The organization:

a. Appoints a SOP/PO accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;

b. Monitors federal privacy laws and policy for changes that affect the privacy program;

c. Allocates an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program;

d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and

f. Updates privacy plan, policies, and procedures, as required to address changing requirements, but at least biennially.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
AR-1 (compliance description)

(compliance description)

The organization has appointed in writing a SOP and PO. Additionally, for organizations external to CMS, an individual shall be identified and appointed in writing that is responsible for compliance with privacy requirements (e.g. a senior privacy official, compliance officers).

Hybrid
AR-3

AR-3 – Privacy Requirements for Contractors and Service Providers

The organization:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Includes privacy requirements in contracts and other acquisition-related documents.

(compliance description)

This includes, but is not limited to, having established privacy roles, responsibilities and access requirements for contractors and service providers and including privacy requirements in all contracts and acquisition-related documents.

Hybrid
SE-2

SE-2 – Privacy Incident Response

The organization:

- a. Develops and implements a Privacy Incident Response Plan; and
- b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

(compliance description)

This includes, but is not limited to, following the requirements for privacy incident response and reporting.

Hybrid
AR-6

AR-6 – Privacy Reporting

The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

(compliance description)

This includes, but is not limited to, providing data as required to CMS for inclusion in reports to higher authorities.

Hybrid
SE-1

SE-1 – Inventory of Personally Identifiable Information

The organization:

a. Establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and

b. Provides each update of the PII inventory to the SOP and the Chief Information Security Officer (CISO) to support the establishment of information security requirements for all new or modified information systems containing PII.

(compliance description)

The CMS Privacy Office will maintain the PII inventory list. This includes, but is not limited to, completing, submitting, being re-validated every 365 days, and having an approved: Privacy Impact Assessment (PIA); and, as applicable, being covered by a current and signed: System of Record Notice (SORN); Computer Matching Agreement (CMA); Memorandum of Agreement (MOA); Memorandum of Understanding (MOU); Letter of Intent (LOI); Interagency Agreement (IA); Information Exchange Agreement (IEA); and, having Data Use Agreement(s) (DUA) in place.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
DI-2

DI-2 – Data Integrity and Data Integrity Board

The organization:

a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

b. Establishes a Data Integrity Board (DIB) when appropriate to oversee organizational CMAs and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

(compliance description)

The organization is subject to an annual review of their program's and/or information system's privacy compliance, which includes an annual security controls assessment (SCA) that addresses that procedures are being followed to validate the integrity of the PII.

Hybrid
AR-4

AR-4 – Privacy Monitoring and Auditing

The organization monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation.

(compliance description)

The organization is subject to an annual review of their program's and/or information system's privacy compliance, which includes an annual SCA for all Privacy control families as listed in the PISP-P.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
AR-2

AR-2 – Privacy Impact and Risk Assessment

The organization:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; and

b. Conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures .

(compliance description)

This includes completing, submitting and having an approved PIA.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
AR-5

AR-5 – Privacy Awareness and Training

The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training at within every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII within every three hundred sixty-five (365) days; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every three hundred sixty-five (365) days.

(compliance description)

This includes: providing privacy awareness and training within 3-working days of individuals having access to CMS PII; providing privacy awareness and training annually thereafter; identifying those individuals who require special privacy role-based training; and, maintaining appropriate training records for all applicable individuals in the organization.

Hybrid
AP-1, AP-2, DM-1

AP-1 – Authority to Collect

The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

AP-2 – Purpose Specification

The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

DM-1 – Minimization of Personally Identifiable Information

The organization:

a. Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, within every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Hybrid
UL-2

UL-2 – Information Sharing with Third Parties

The organization:

a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes;

b. Where appropriate, enters into MOUs, LOIs, CMAs, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

(compliance description)

This includes, but is not limited to, completing, submitting, being re-validated every 365 days, and having an approved: PIA; and, as applicable, being covered by a current and signed: SORN; CMA; MOA; MOU; LOI; IA; IEA; and, having DUAs in place.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
TR-1

TR-1 – Privacy Notice

The organization:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Hybrid
TR-1 compliance description

(compliance description)

This includes, but is not limited to, completing, submitting, being re-validated every 365 days, and having an approved: PIA; and, as applicable, being covered by a current and signed: SORN; CMA; MOA; MOU; LOI; IA; IEA; and, having DUAs in place; and if applicable, provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
TR-1(1)

TR-1(1) - Real-Time or Layered Notice – Enhancement

The organization provides real-time and/or layered notice when it collects PII.

(compliance description)

This includes, but is not limited to, completing, submitting, being re-validated every 365 days, and having an approved: PIA; and, as applicable, being covered by a current and signed: SORN; CMA; MOA; MOU; LOI; IA; IEA; and, having DUAs in place; and if applicable, provides real-time and/or layered notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

Hybrid
TR-2

TR-2 – System of Records Notices and Privacy Act Statements

The organization:

a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;

b. Keeps SORNs current; and

c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

(compliance description)

This includes, but is not limited to, being covered by an established SORN, if applicable, and that has been re-validating every 365 days; and if applicable, provides notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
AR-8

AR-8 – Accounting of Disclosures

The organization:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:

(1) Date, nature, and purpose of each disclosure of a record; and

(2) Name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or a minimum of five (5) years after the disclosure is made, whichever is longer; and

c. Makes the accounting of disclosures available to the person named in the record upon request.

(compliance description)

This includes, but is not limited to having DUAs in place.

Hybrid
AR-7, DM-1(1) and DM-2(1)

AR-7 – Privacy-Enhanced System Design and Development

The organization designs information systems to support privacy by automating privacy controls.

DM-1(1) - Locate/Remove/Redact/Anonymize PII – Enhancement

The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

DM-2(1) - System Configuration – Enhancement

The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Hybrid
DM-3 and DM-3(1)

DM-3 – Minimization of PII Used in Testing, Training, and Research

The organization:

a. Develops policies and procedures that minimize the use of PII for testing, training, and research; and

b. Implements controls to protect PII used for testing, training, and research.

DM-3(1) - Risk Minimization Techniques – Enhancement

The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

(compliance description)

This includes the privacy artifacts required in the CMS eXpedited Life Cycle (XLC) and highlighted in the *Privacy-Enhanced System Design and Development* section of the RMH for Privacy.

Hybrid
DI-1 and DI-1(1)

DI-1 – Data Quality

The organization:

a. Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

b. Collects PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the DIB; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

DI-1(1) - Validate PII – Enhancement

The organization requests that the individual or individual's authorized representative validate PII during the collection process.

Hybrid
DI-1 and DI-1(1) compliance description

(compliance description)

This includes the following:

a. Confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

b. Collects PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the DHHS DIB; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Hybrid
DI-1(2)

DI-1(2) - Re-Validate PII – Enhancement

The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate as directed by the DHHS DIB.

The organization's program's and/or information system's must adhere to the CMS RMH for Privacy, Privacy-Enhanced System Design and Development section of the RMH for Privacy, which requires the following actions at least every 365 days:

a. Re-validates to the greatest extent practicable, the personally identifiable information (PII) data collected is accurate, relevant, timely, and complete;

b. Re-validates PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the DHHS DIB; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
IP-1

IP-1 – Consent

The organization:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Hybrid
IP-1 compliance description

(compliance description)

This includes the program or information system implementing mechanisms to support itemized or tiered consent for specific uses of data, which includes:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Hybrid
IP-1(1)

IP-1(1) - Mechanisms Supporting Itemized or Tiered Consent – Enhancement

The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

(compliance description)

The program and/or information system develops processes and procedures for implementing mechanisms to support itemized or tiered consent for specific uses of data.

Hybrid
IP-2

IP-2 – Individual Access

The organization:

a. Provides individuals the ability to have access to their PII maintained in its system(s) of records;

b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

c. Publishes access procedures in SORNs; and

d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

(compliance description)

The program and/or information system develops processes and procedures for individuals to have access to their individual information.

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Hybrid
IP-3

IP-3 – Redress

The organization:

a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and

b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

(compliance description)

The program and/or information system develops processes and procedures for implementing mechanisms to support redress activities to ensure individual PII is accurate and amendable when required.

IP-4 – Complaint Management

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

(compliance description)

The program and/or information system develops processes and procedures for receiving and responding to complaints from individuals, and reporting these complaints to the CMS PO.

Hybrid
IP-4(1)

IP-4(1) - Response Times – Enhancement

The organization responds to complaints, concerns, or questions from individuals within the CMS-defined time period.

(compliance description)

The program and/or information system fully inherits the Response Times established by the CMS PO and CMS SOP. For organizations external to CMS, procedures for Response Times are defined and included in the contract/agreement under which CMS engages the external organization, and must be adhered to by the organization. The external organization must formally adopt the Response Times policies into the practices of the organizational segment performing work on behalf of CMS.

Hybrid
UL-1

UL-1 – Internal Use

The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

(compliance description)

This is a hybrid control. In order to inherit this control, individual program officials and IT system managers shall ensure that the use of records, including those that contain PII, by CMS employees or business partners of the agency, are only used on a need to know basis.

Hybrid
DM-2

DM-2 – Data Retention and Disposal

The organization:

a. Retains each collection of PII for minimum allowable necessary to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

(compliance description)

This includes following the procedures required under NARA and the CMS Records Management Schedule.

Effective Date of Implementation

- April 30, 2014
- SCAs begin addressing all privacy controls
- Findings in CMS FISMA Audit Tracking System (CFACTS)
- POA&Ms & CAPs required

HELP !!!

- www.cms.gov/Privacy
  - Link for Privacy Impact Assessments
  - List of System of Record Notices (SORN)
  - List of Computer Matching Agreements (CMA)
  - Data Use Agreement (DUA) Procedures
- Email resources
  - Privacy Impact Assessments PIA@cms.hhs.gov
  - Data Use Agreements DataUseAgreement@cms.hhs.gov
  - All other Privacy questions Privacy@cms.hhs.gov