Crosswalking the DMP to the DMP SAQ

For organizations using an approved DMP as a starting point when transitioning to the DMP SAQ

Referencing Your DMP to Complete the DMP SAQ

The Data Management Plan (DMP) requirement for CMS Data Use Agreement (DUA) for Research Identifiable Files (RIF) has been updated. The new DMP, a DMP Self-Attestation Questionnaire (SAQ), reflects the security and privacy provisions outlined in the CMS Acceptable Risk Safeguards (ARS) 3.1 data security framework.

The below table provides a reference for how organizations may refer to their approved DMP as a starting point to complete the new DMP SAQ. The table maps the DMP SAQ to the DMP in the order the questions are presented in the DMP SAQ.

The DMP SAQ includes new questions and requirements not previously included in the DMP. Therefore, not all DMP SAQ questions map to the DMP. Guidance for DMP SAQ questions not listed in the crosswalk below can be found using the CMS ARS v3.1 publication or DMP SAQ Requirements & Guidance for Security & Privacy Controls document.

Control Family	DMP SAQ Question # / Control #	DMP Question # / Section
Access Control	*1.1 (AC-01 control)*	*1.4 (Staffing)* *2.4 (Access Management)*
Access Control	*1.2 (AC-02 control)*	*2.4 (Access Management)* *4.2 (Access Termination)*
Access Control	*1.3 (AC-04 control)*	*2.4 (Access Management)* *2.1 (Data Sharing)*
Access Control	*1.4 (AC-21 control)*	*2.1 (Data Sharing)* *2.4 (Access Management)*
Access Control	*1.5 (AC-03 control)*	*2.4 (Access Management)* *1.9 (Logical Access)*
Access Control	*1.6 (AC-05 control)*	*2.4 (Access Management)*
Access Control	*1.7 (AC-06, AC-06(01), AC-06(09) controls)*	*2.4 (Access Management)*
Access Control	*1.8 (AC-07 control)*	*2.4 (Access Management)* *2.5 (Login Requirements)*
Access Control	*1.9 (AC-08 control)*	*2.4 (Access Management)*
Access Control	*1.10 (AC-11 control)*	*2.4 (Access Management)* *2.5 (Session Timeouts)*
Access Control	*1.11 (AC-14 control)*	*2.4 (Access Management)*

Control Family	DMP SAQ Question # / Control #	DMP Question # / Section
Access Control	*1.12 (AC-17 controls)*	*2.4 (Access Management)*
Access Control	*1.13 (AC-18, AC-18(01) controls)*	*2.4 (Access Management)* *2.5 (Encryption)*
Access Control	*1.14 (AC-20, AC-20(01), AC-20(02)) controls*	*2.1 (Data Sharing)* *2.4 (Access Management)*
Access Control	*1.15 (AC-21 control)*	*2.1 (Data Sharing)* *2.4 (Access Management)*
Awareness and Training Control	*2.1 (AT-02 control)*	*1.5 (Awareness & Training)*
Awareness and Training Control	*2.2 (AT-03 control)*	*1.5 (Awareness & Training)*
Audit and Accountability Control	*3.3 (AU-03, AU-03(01) controls)*	*2.2 (Data Tracking System)*
Audit and Accountability Control	*3.9 (AU-09 control)*	*2.5 (Encryption)*
Security Assessment and Authorization Control	*4.1 (CA-01 control)*	*3.2 (Annual Security Review)*
Security Assessment and Authorization Control	*4.2 (CA-03, CA-03(05), CA-09 controls)*	*2.1 (Data Sharing)* *3.3 (Updates of Plans and Procedures)*
Security Assessment and Authorization Control	*4.3 (CA-03(05) control)*	*1.8 (Tracking & Team Access)*
Security Assessment and Authorization Control	*4.4 (CA-07 control)*	*3.2 (Annual Security Review)*
Configuration Management Control	*5.1 (CM-01 control)*	*1.6 (Infrastructure)*
Configuration Management Control	*5.2 (CM-03 control)*	*1.6 (Infrastructure)*
Configuration Management Control	*5.3 (CM-06 control)*	*1.6 (Infrastructure)*
Configuration Management Control	*5.4 (CM-02 control)*	*1.6 (Infrastructure)*
Configuration Management Control	*5.5 (CM-05 control)*	*1.6 (Infrastructure)* *1.7 (Physical Control)* *1.9 (Physical and Logical Access)*
Configuration Management Control	*5.6 (CM-07 control)*	*1.6 (Infrastructure)*
Configuration Management Control	*5.7 (CM-08, CM-08(01) controls)*	*1.6 (Infrastructure)*

Control Family	DMP SAQ Question # / Control #	DMP Question # / Section
Configuration Management Control Continued	*5.8 (CM-11 control)*	*1.6 (Infrastructure)*
Identification and Authentication Control	*7.2 (IA-02, IA-03, IA-05 controls)*	*2.5 (Password Protocols)* *2.5 (Encryption)*
Incident Response Control	*8.1 – 8.7 (IR-01, IR-02, IR-04, IR-05, IR-06, IR-07, IR-08 controls)*	*3.1 (Incident Response)*
Media Protection Control	*10.3 (MP-04, MP-06 controls)*	*2.3 (Physical Transport or Removal)* *4.1 (Disposition/Destruction of Data)*
Media Protection Control	*10.4 (MP-05 control)*	*1.7 (Physical Control)* *2.2 (Data Tracking System)* *2.3 (Physical Transport or Removal)*
Media Protection Control	*10.5 (MP-06, MP-06(01) controls)*	*2.2 (Data Tracking System)* *4.1 (Disposition/Destruction of Data)*
Media Protection Control	*10.6 (MP-07 control)*	*2.3 (Physical Transport or Removal)* *4.4 (Disposition Methods)*
Media Protection Control	*10.7 (MP-07 control)*	*2.3 (Physical Transport or Removal)* *4.4 (Disposition Methods)*
Media Protection Control	*10.8 (MP-CMS-01 control)*	*4.1 (Disposition/Destruction of Data)* *4.4 (Disposition Methods)*
Physical and Environmental Control	*11.1 (PE-01 control)*	*1.7 (Physical Control)* *1.9 (Physical Safeguards)* *2.3 (Physical Transport or Removal)*
Physical and Environmental Control	*11.2 (PE-02 control)*	*1.7 (Physical Control)* *1.9 (Physical Safeguards)* *2.3 (Physical Transport or Removal)*
Physical and Environmental Control	*11.3 (PE-03 control)*	*1.7 (Physical Control)* *1.9 (Physical Safeguards)* *2.3 (Physical Transport or Removal)*
Planning Control	*12.1 (PL-02 control)*	*3.2 (Annual Security Review)* *3.3 (Updates of Plans and Procedures)*
Planning Control	*12.2 (PL-04 control)*	*1.3 (Binding Agreements)*
Personnel Security Control	*13.1 (PS-03 control)*	*1.4 (Staffing)* *1.8 (Tracking & Team Access)*
Personnel Security Control	*13.2 (PS-04 control)*	*1.4 (Staffing)* *1.8 (Tracking & Team Access)* *4.1 (Disposition/Destruction of Data)* *4.2 (Access Termination)* *4.4 (Disposition Methods)*

Control Family	DMP SAQ Question # / Control #	DMP Question # / Section
Personnel Security Control	*13.3 (PS-03 control)*	*1.4 (Staffing)* *1.8 (Tracking & Team Access)*
Personnel Security Control	*13.4 (PS-06 control)*	*1.3 (Binding Agreements)* *1.8 (Tracking & Team Access)*
Personnel Security Control	*13.5 (PS-07 control)*	*1.8 (Tracking & Team Access)*
Personnel Security Control	*13.6 (PS-08 control)*	*1.8 (Tracking & Team Access)*
System and Communications Protection Control	*16.2 (SC-08, SC-13, SC-28 controls)*	*2.3 (Physical Transport or Removal)* *2.5 (Encryption)*
System and Communications Protection Control	*16.4 (SC-10 control)*	*2.5 (Session Timeouts)*
System and Information Integrity Control	*17.7 (SI-10 control)*	*2.5 (Password Protocols)*
System and Communications Protection Control	*17.8 (SI-12 control)*	*4.4 (Disposition Methods)*
Program Management Control	*18.1 (PM-02 control)*	*1.1 (Physical Possession)*
Accountability, Audit and Risk Management	*19.1 (AR-01 control)*	*3.3 (Updates of Plans and Procedures)*
Accountability, Audit and Risk Management	*19.3 (AR-04 control)*	*3.3 (Updates of Plans and Procedures)*
Accountability, Audit and Risk Management	*19.4 (AR-05(a) control)*	*1.5 (Awareness & Training)*
Accountability, Audit and Risk Management	*19.5 (AR-05(b)(c) control)*	*1.5 (Awareness & Training)* *1.3 (Binding Agreements)*
Accountability, Audit and Risk Management	*19.6 (AR-08 control)*	*1.8 (Tracking & Team Access)*
Security	*24.1 (SE-CMS-01)*	*1.2 (Inventory)*
Use Limitation	*26.2 (UL-01, UL-02(a)(b) controls)*	*2.1 (Data Sharing)*
Use Limitation	*26.3 (UL-02(c)(d) controls)*	*2.1 (Data Sharing)*

This document is provided by the Data Privacy Safeguard Program. MBL Technologies is the authorized CMS contractor and can be reached for questions or additional assistance at DPSP@cms.hhs.gov.