

DATA PRIVACY SAFEGUARD PROGRAM

DATA MANAGEMENT PLAN SELF-ATTESTATION QUESTIONNAIRE (DMP SAQ)

PURPOSE: The CMS data your organization is requesting contains sensitive information that requires evidence that adequate data security and privacy safeguards are in place to protect the confidentiality, integrity, and availability of CMS data. The following questionnaire will support your organization in attesting and demonstrating your compliance with CMS safeguard requirements, specifically the [CMS Acceptable Risk Safeguards \(ARS\) 3.1 Publication](#).

1. DUA ORGANIZATION INFORMATION

| | |
|-------------------------------|--|
| REQUESTING ORGANIZATION | The Curators of the University of Missouri |
| COMPUTING ENVIRONMENT NAME | Amazon AWS server instance |
| COMPUTING ENVIRONMENT TYPE | <input checked="" type="checkbox"/> Cloud Service Provider (CSP) <input type="checkbox"/> Onsite <input type="checkbox"/> Hybrid: Uses CSP & Exists Onsite |
| COMPUTING ENVIRONMENT ADDRESS | US-EAST-2 (Ohio) |

2. DATA CUSTODIAN

The Data Custodian is the individual who will be responsible for the observance of all the conditions of use for the environment identified in this document, including the establishment and maintenance of security arrangements to prevent unauthorized use. The Data Custodian must sign the DMP SAQ (in section 6) prior to submission. Please note that the DMP SAQ only allows for a single Data Custodian.

| | |
|-------------------------------|--|
| DATA CUSTODIAN | Dr. Lemuel R. Waitman, Associate Dean of Informatics, University of Missouri |
| DATA CUSTODIAN OFFICE ADDRESS | CE707 Clinical Support & Education Building, DC006.00, Columbia, MO 65212 |
| DATA CUSTODIAN PHONE NUMBER | 573-882-2190 |
| DATA CUSTODIAN EMAIL ADDRESS | russ.waitman@health.missouri.edu |

PRA Disclosure Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is **0938-1411 (Expires 10/31/2025)**. This is a **required to retain or obtain a benefit** information collection. The time required to complete this information collection is estimated to average **90 minutes** per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850. ******CMS Disclosure**** Please do not send applications, claims, payments, medical records or any documents containing sensitive information to the PRA Reports Clearance Office. Please note that any correspondence not pertaining to the information collection burden approved under the associated OMB control number listed on this form will not be reviewed, forwarded, or retained. If you have questions or concerns regarding where to submit your documents, please contact DataUseAgreement@cms.hhs.gov.**

Please provide the information for a secondary Point of Contact (POC) in the event the Data Custodian changes or cannot be reached.

| | |
|------------------------------------|---|
| SECONDARY POC | Dr. Xing Song, Assistant Professor of Health Management and Informatics |
| SECONDARY POC PHONE NUMBER | 573-882-1352 |
| SECONDARY POC EMAIL ADDRESS | CE738 Clinical Support & Education Building, Columbia, MO 65212 |

3. INSTRUCTIONS FOR COMPLETING THE DMP SAQ

The DMP SAQ contains security and privacy controls based on the [CMS Acceptable Risk Safeguards 3.1 Publication](#), which uses NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* control reference structure. Please note that below each question the [CMS Acceptable Risk Safeguards 3.1 Publication](#) safeguard number has been provided for reference, if additional guidance is needed.

For Section 4 (Security Controls): A security control is defined as an operational, technical, or management safeguard or countermeasure used by an information system or an organization to maintain the integrity, confidentiality, and availability of its information.

- For each question, in Part A (i.e., 1A, 2A, etc.), please:
 - Answer “Yes” if the security control is documented in a policy or procedure and all elements of the question are satisfied.
 - Answer “No” if the security control is not documented in a policy or procedure or if all elements of the question are not satisfied.
- In Part A, please note that a rationale is required for both “Yes” and “No” responses.
 - If “Yes,” please cite the documentation and describe the capability.
 - If “No,” please provide a rationale and any compensating control(s) in effect.
- In Part B, please note that a rationale is optional.
- **Rationale and policies:** A rationale or policy reference is required for all Part A questions in Section 4. Please note that a rationale is optional for all Part B questions. A rationale should reference or describe the method by which a control will be addressed by the DUA requesting organization or indicate the compensating security control(s) in place. The National Institute of Standards and Technology (NIST) defines a compensating security control as a management, operational, or technical control used by an organization instead of a recommended security control that provides equivalent or comparable protection for an information system.

For Section 5 (Privacy Controls): As defined by the National Institute of Standards and Technology (NIST), a privacy control is an administrative, technical, and physical safeguard employed within an organization to protect and ensure the proper handling of PII or prevent activities that create privacy risks.


- For this section, provide an attestation of “Yes” or “No” if the control has been implemented at your organization. Please note that none of the questions require a rationale, any rationale provided in Section 5 is optional.

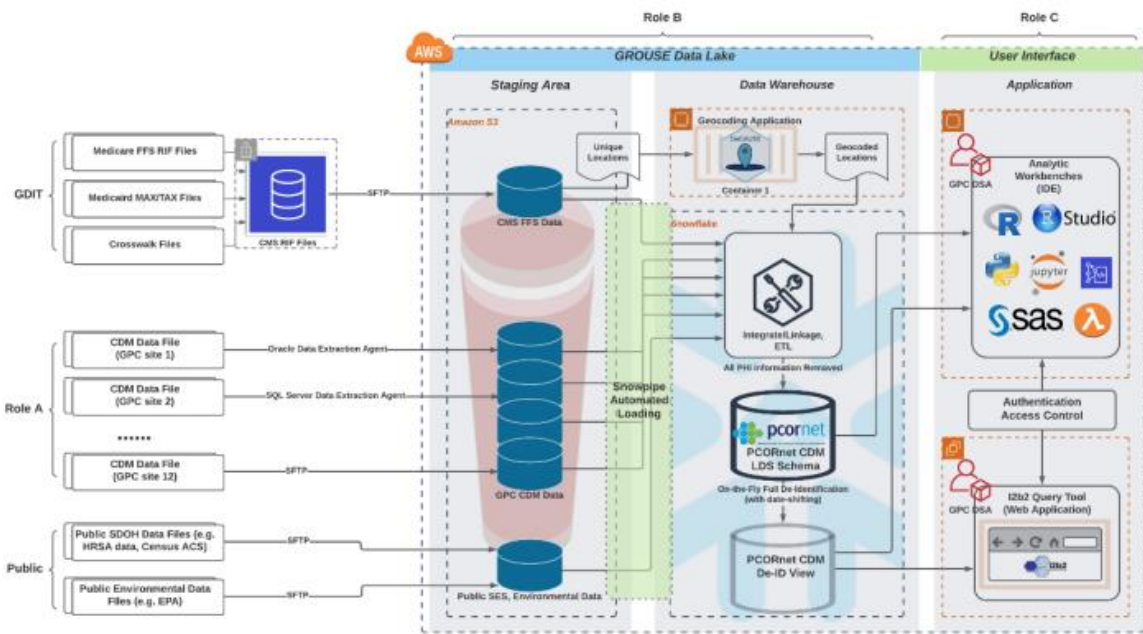
GUIDANCE: For supplementary guidance on the CMS ARS requirements for privacy and security controls, please refer to the [Data Management Plan Self-Attestation Questionnaire \(DMP SAQ\): Requirements & Guidance for Security & Privacy Controls](#).

4. SECURITY CONTROLS

1A. Access Controls: Attestation and Rationale

| # | Question | Response |
|-----|---|--|
| 1.1 | <p>Does your organization have an access control policy that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and DUA compliance by all research parties using CMS data?</p> <p>(ARS v3.1 AC-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>CMS data access control policy will follow the Data Classification Level (DCL) system (https://www.umsystem.edu/ums/is/infosec/classification#) reinforced at University of Missouri (MU): a) Raw CMS data will be treated as DCL4 (“highly restricted”); b) limited CMS data with only real dates will be treated as DCL3 (“restricted”); c) the fully deidentified data following well-established “safe harbor” methods will be treated as DCL2 (“sensitive”); d) Only aggregated data with cell counts above 10 that are approved to be used for publication or public dissemination will be treated as DCL1 (“public”). Regulations, laws and standards that affect data in different DCL tiers include, but are not limited to, the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), the Export Administration Regulations (15 CFR 730 et seq.), the Health Insurance Portability & Accountability Act (HIPAA) and Payment Card Industry (PCI) standards. These regulation, laws and standards thoroughly address the purpose, scope, responsibility, management commitment, coordination among organizational entities, and DUA compliance associated with different DCL level. Any research activities must be conducted in accordance with this code of conduct https://www.muhealth.org/sites/default/files/PDFs/20-0319IC_CodeofConduct-update_FINALv2.pdf) and any professional ethical codes applicable to the research activities. Request and oversight for research activities is submitted to applicable Institutional Review Boards (IRBs). In addition, we have developed a full suite of policy and procedures following best practices and NIST-800-53r4 controls from the AC family, which requires an annual review and update (as well as spontaneous review when critical changes is needed).</p> | |
| 1.2 | <p>Does your organization’s account management system assign an account manager, ensure unique user accounts, ensure group/role conditions for membership, and review user accounts periodically?</p> <p>(ARS v3.1 AC-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Each user will be assigned with a unique user account, which is associated to a pre-defined project-specific Role (A, B, C) with different level of privileges approved by key stakeholders. A project account manager (Role B Administrator) is assigned and trained with ongoing responsibilities to monitor accounts regularly as well as review accounts at least annually. The account manager is responsible to:</p> <ol style="list-style-type: none"> 1. Work closely with key stakeholders and Institutional Review Board (IRB) to oversight account provisioning and continuous monitoring. 2. Ensure access to the system is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | |

| # | Question | Response |
|---|--|----------|
| | <ol style="list-style-type: none"> Ensure access to the system is limited to the types of transactions and functions that authorized users are permitted to execute. Identify distinct account types (i.e., individual, group, system, application, guest/anonymous, and temporary). Enable a centralized and automated account management with at least one “account manager” appointed and properly trained. Establish conditions and policies for group and role membership. Identify authorized users of the information asset and specifying access privileges for each account. Require appropriate approvals for requests to establish accounts. Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions. Establish, activate, modify, disable, and remove accounts in accordance with defined procedures. Monitors the use of information system accounts (e.g. user accounts). Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. Not allow the use of guest/anonymous and temporary accounts. Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes. Deactivate/disable emergency, temporary and expired accounts that are no longer required and accounts of terminated or transferred users. Tracks all types of account changes (e.g. creation, enabling, modifying, disabling, deletion) within audit records without interruptions. <p>GROUSE account governance process is described in the figure below:</p>  | |

| # | Question | Response |
|-----|--|--|
| | <p>Within the AWS environment, we adopt the native federation solution, single-sign-on (SSO), for better central account management, which uses AWS SSO identity store as default identify source. We define Permission Sets (a collection of administrator-defined policies that AWS SSO uses to determine a user's effective permissions) to consistently and programmatically enforce access controls (allow or deny) associated with users' roles and accounts.</p> | |
| 1.3 | <p>Does your organization ensure it controls information flow within the system and any interconnected (internal or external) systems? Please describe where the information is coming from and where it is going.</p> <p>(ARS v3.1 AC-04)</p> | <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> |
| | <p>Data comes from CMS data provider (GDIT) and participating sites within the GPC network under agreement. On top of existing safeguards on data encryption at rest and during transmission leveraging both client-side and server-side encryption provided by AWS, the MU-NextGenBMI team also has established governance process to make sure only aggregated data (adhere to CMS' current cell size suppression policy) can be shared outside the system upon approval. All these technical and administrative safeguards will provide the foundation that meets and/or exceeds the security requirements established by the Office of Management and Budget (OMB), Federal Information Processing Standard 200 (FIPS), and NIST 800-53 special publication entitled, "Recommended Security Controls for Federal Information Systems". Authorized Role-B users ("Administrators") will have access to the raw data files (DCL-4) which is treated with the highest protection, while Authorized Role-C users ("Analysts") will have access to the corresponding limited or de-identified version of the dataset.</p>  <p>The diagram illustrates the data architecture for the GPC network. It shows data sources on the left (GDIT, Role A, Public) feeding into a central 'GROUSE Data Lake' (AWS S3) via SFTP. The data lake is divided into a 'Staging Area' and a 'Data Warehouse'. Data flows from the staging area through a 'Geocoding Application' and 'Integrated Linkage, ETL' to the data warehouse. The data warehouse contains 'PCORnet CDM LDS Schema' and 'PCORnet CDM De-ID View'. Data is then accessed by Role B (Administrators) and Role C (Analysts) through a 'User Interface' which includes 'Analytic Workbenches (IDE)' and 'Authentication Access Control'.</p> | |

| # | Question | Response |
|-----|--|--|
| 1.4 | Does your organization have a process for approved information-sharing circumstances that determines what is shared with external users (e.g. collaborators) and ensures that access authorizations assigned to these users aligns with the organization's access restrictions? (ARS v3.1 AC-21) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>No line items (i.e., beneficiary-level or patient-level data) can be shared outside of the approved research team (Stakeholder, Role-B, Role-C). Only aggregated, de-identified results from the study can be used to either shared with PCORnet (https://pcornet.org/) coordinating center (funding agency) for quality control purpose or target for publication in peer-reviewed journals for each of the cohorts and the informatics methods employed. Prior to publication, the results may be presented at a national or international scientific meeting, such as the annual AMIA Joint Summits on Translational Science, Association for Clinical and Translational Science, San Antonio Breast Cancer Symposium, and the American Association of Neuromuscular & Electrodiagnostic Medicine Annual Meeting. We strictly adhere to the CMS' current cell size suppression policy, that is: "Any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 5 or any data derived from such files) must adhere to CMS' current cell size suppression policy. This policy stipulates that no cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less". All research team members are bound by the Data Sharing Agreement (DSA) and GPC External Collaborator Agreement among Greater Plain Collaborative (GPC, https://www.gpcnetwork.org/) institutions with explicit policies regarding restricted data sharing. On the other hand, the analytic methods and code developed to support PCORnet will be shared as open source materials on our GPC websites to facilitate adoption and dissemination with the PCORnet and potential investigators who might use the PCORnet resource.</p> | |

1B. Access Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 1.5 | Does your organization use logical access controls (e.g., roles, groups, file permissions) to restrict access to information? (ARS v3.1 AC-03) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.6 | Does your organization's information system separate users based on their duties (e.g., users, researchers, management, etc.)? (ARS v3.1 AC-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.7 | Does your organization ensure that only authorized users have permissions required to perform their job functions by disabling non-essential functions and removable media devices; ensure security functions are explicitly authorized; | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|------|--|--|
| | <p>ensure that authorized users utilize their own account to access the system; escalate privileges to perform administrative functions; and audit all privileged account usage activities?</p> <p>(ARS v3.1 AC-06, AC-06(01), AC-06(09))</p> | |
| | Click here to enter text (<i>Optional</i>). | |
| 1.8 | <p>Does your organization's information system automatically disable accounts after a defined number of consecutive failed login attempts? For systems that contain PII/PHI, when the limit of attempts is exceeded a system administrator intervention is required.</p> <p>(ARS v3.1 AC-07)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.9 | <p>Does your organization's information system display a notification or banner before granting access to the information systems?</p> <p>(ARS v3.1 AC-08)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.10 | <p>Does your organization's information system lock user sessions after an organization defined time limit of non-use and/or are automatically disconnected under specified circumstances?</p> <p>(ARS v3.1 AC-11)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.11 | <p>Does your organization's information system define actions that can be taken on the system without authentication (e.g., viewing certain webpages with public information only or generic information)?</p> <p>(ARS v3.1 AC-14)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.12 | <p>Does your organization's remote connections have usage restrictions; have connection requirements such as cryptography connected to managed network access control points; have guidelines for user access; are monitored through audit records; and explicitly authorize the usage of privileged commands through the remote connection?</p> <p>(ARS v3.1 AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04))</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

| # | Question | Response |
|------|--|--|
| 1.13 | Does your organization have usage restrictions and implementation guidance (e.g., encryption, EAP, LEAP, etc.) for wireless access and/or mobile devices? (ARS v3.1 AC-18, AC-18(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.14 | Does your organization ensure that the information system does not allow systems outside of the its authorization boundary to store, transmit, or view system information? (ARS v3.1 AC-20, AC-20(01), AC-20(02)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 1.15 | Does your organization have a process for determining what is shared with external users (e.g. collaborators)? (ARS v3.1 AC-21) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

2A. Awareness and Training Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 2.1 | Does your organization ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems and how? (ARS v3.1 AT-02) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We require all users of the system where CMS data is to go through trainings consist of the following 4 components:</p> <ol style="list-style-type: none"> 1. CITI training on Human Subjects Research (https://about.citiprogram.org/en/series/human-subjects-research-hsr/). 2. A consistent security and privacy awareness training provided by NIH (https://irtsectraining.nih.gov/publicUser.aspx) on top of the mandatory institutional security awareness trainings. 3. The policy and procedure deck (i.e. System Security Plan, or SSP) that we have developed specifically for this cloud-based information system where CMS data is stored and processed to be accessible. Security-related duties and responsibilities associated with the role assigned to the “trainee” personnel are clearly defined in this SSP (the “Overview” section). 4. 4. Insider Threat Brochure which has been used previously. | |

| # | Question | Response |
|-----|--|--|
| 2.2 | <p>Does your organization ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities prior to them assuming their security-specific roles and responsibilities? Do they receive additional training based on system changes (e.g., statute, regulation or policy changes) and at least once a year for refreshed role-based security awareness training?</p> <p>(ARS v3.1 AT-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Each personnel are required to go through training (described in Q2.1, AT-2) which include sufficient information on information security-related duties and responsibilities in general and associated with the user's role. Role-B administrators (Account admin and System admin) will track and collect all required training records from personnel before access can be granted. Additional training is required at least annually or there are any major system changes (e.g., statute, regulation or policy changes).</p> | |

2B. Awareness and Training Controls

Please note that there are no questions in this control family that require an attestation. Please proceed to 3A.

3A. Auditing and Accountability Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 3.1 | <p>Does your organization have a policy for audit and accountability tasks to provide auditable evidence for system transactions on chance that an information system crashes, is hacked, or some other issue that disables the system?</p> <p>(ARS v3.1 AU-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We have developed a full suite of policy and procedures following best practices and NIST-800-53r4 controls from the AU family, which requires an annual review and update (as well as spontaneous review when critical changes is needed).</p> | |
| 3.2 | <p>Does your organization have the capability to audit events on the information system including:</p> <p>User logon and logoff (successful and unsuccessful); all system administration activities; modification of privileges and access; application alerts and error messages; configuration changes, account creation; modification or deletion; concurrent logon from different work stations; override of access control mechanisms; startup/shutdown of audit logging services; and audit logging service configuration changes?</p> <p>(ARS v3.1 AU-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We leverage multiple AWS managed services (AWS CloudTrail, AWS CloudWatch, AWS Config) to capture loggings for all required audit events, including but not limited to:</p> <ol style="list-style-type: none"> 1. User successful and unsuccessful logon; 2. Modification of privileges and access; 3. Application alerts and error messages; 4. All configuration and rule changes; 5. Account creation; modification or deletion; | |

| # | Question | Response |
|-----|--|--|
| | <p>6. Startup/shutdown of audit logging services as well as policies that prevent shutdown of audit logging services;</p> <p>7. Any audit logging service configuration changes;</p> <p>We have also implemented mandatory guardrails/controls to ensure that loggings of these audit events should not be interrupted. Any attempt to shut down or change audit logging services will be immediately detected and alerts will be sent to Role-B administrators.</p> | |
| 3.3 | <p>Does your organization ensure that the audit records from the information system contain the following metadata to support the detection, monitoring, investigation, response, and remediation of security and privacy incidents:</p> <p>Date and time of the event (e.g., a timestamp); process identifier or system component (e.g., software, hardware) generating the event; user or account that initiated the event (unique username/identifier); event type; event outcome (succeed/failure); any privileged system functions executed; process creation information (command line captures if applicable)?</p> <p>(ARS v3.1 AU-03, AU-03(01))</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>All required metadata to support the detection, monitoring, investigation, response and remediations of security and privacy incidents as required above is recorded and reported by AWS audit logging services (e.g., AWS CloudTrail). In addition, for any security and privacy incidents detected, AWS also provides detailed recommendations on how to investigate, response and remediate the issues.</p> | |

3B. Auditing and Accountability Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 3.4 | <p>Does your organization ensure adequate storage capacity for 90 days of audit records?</p> <p>(ARS v3.1 AU-04, AU-11)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Click here to enter text (Optional).</p> | |
| 3.5 | <p>Does your organization ensure that administrators are notified of process failures through the audit process of the information systems?</p> <p>(ARS v3.1 AU-05)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Click here to enter text (Optional).</p> | |
| 3.6 | <p>Does your organization ensure that:</p> <p>Audit records are reviewed weekly and manually every 30 days; system logs, network utilization/traffic, security software, and alerts are reviewed daily; automated audit record analysis is used to review audit records; automated audit record analysis is correlated across the organization; and administrator groups logs are inspected at least every 14 days to ensure unauthorized administrator, system, and privileged application accounts have not been created?</p> <p>(ARS v3.1 AU-06, AU-06(03))</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Click here to enter text (Optional).</p> | |

| # | Question | Response |
|------|--|--|
| 3.7 | Does your organization ensure audit records are searchable? (ARS v3.1 AU-07(01), AU-07(02)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 3.8 | Does your organization ensure the internal system clocks of the information systems are regularly synchronized with a common authoritative time source (e.g. Atomic clocks, external NTP server, NIST time service, etc.) and that audit records use the internal system clocks to generate a time stamp? (ARS v3.1 AU-08, AU-08(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 3.9 | Does your organization ensure the audit records and tools are protected from unauthorized access, deletion and modification? Is access to these audit records limited to a subset of privileged users? (ARS v3.1 AU-09, AU-09(04)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 3.10 | Does your organization ensure that audit records are retained for 90 days in “hot” storage and retained for one (1) year in archive storage? (ARS v3.1 AU-11) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

4A. Security Assessment and Authorization Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 4.1 | Does your organization have a policy for security assessment and authorization activities? (ARS v3.1 CA-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have developed a full suite of policy and procedures following best practices and relevant NIST-800- 53r4 controls from the CA family, which requires an annual review and update (as well as spontaneous review when critical changes is needed). | |
| 4.2 | Does your organization ensure that any external and internal interconnections, if applicable, have documented authorization decisions for connections from the system to other systems using some form of agreement (MOU, MOA, ISA, etc.); document the interface, security requirements, and type of information exchanged; and establish timeframes for reviewing and updating ISAs? (ARS v3.1 CA-03, CA-03(05), CA-09) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have an established business associate contract (BAA) and statement of work (SOW) among DLT, AWS ProServ and University of Missouri, which specifies the responsibilities of each party. As written in the “Security” and “Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Obligations” of the agreement, DLT is certified as compliant with ISO 27001 | |

| # | Question | Response |
|-----|---|--|
| | <p>and required to provide HIPAA compliant account for this project. DLT agrees to not access any of our data except for the billing information. In execution, we have been provisioned with “FullAWSAccess” privilege in our AWS Organization account to set up all necessary controls in compliance with NIST-800-53r4 set forth in this DMP SAQ, including necessary detective and preventive controls against the management account held by DLT.</p> <p>We also have an established BAA with Snowflake Inc. (https://www.snowflake.com/), as we have chosen Snowflake as our data warehouse solution through SaaS. Snowflake is built on AWS VPC which is connected with the rest of our AWS Organization components, especially AWS S3 buckets. Data staged on the private S3 bucket will be transferred to Snowflake data warehouse via Snowpipe (https://docs.snowflake.com/en/user-guide/data-load-snowpipe-intro.html) using client-side encryption for further transformation, curation and de-identification. Following the “least privilege” principle, we will only assign Snowflake “reading” and “listing” rights to the S3 bucket endpoint.</p> | |
| 4.3 | <p>Does your organization use a deny-all, permit-by-exception policy for system access to ensure that only those connections which are essential and approved are allowed? (ARS v3.1 CA-03(05))</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>AWS IAM strictly follows a logic of Explicit deny > Explicit Allow > Implicit Deny (at default). In other words, any IAM user will start with no permission to access any services (enforced by config rule) until an explicit permission is assigned to the user account, which can be overridden by an explicit deny. All users also abide by higher-level mandatory service control policies (SCP) or Guardrails (for example, none of them is allowed to delete any audit logs).</p> | |

4B. Security Assessment and Authorization Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 4.4 | <p>Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation and ongoing security assessments? (ARS v3.1 CA-07)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Click here to enter text (<i>Optional</i>).</p> | |

5A. Configuration Management Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 5.1 | <p>Does your organization have a policy for configuration management that is reviewed/updated at least once a year? (ARS v3.1 CM-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We have developed a full suite of policy and procedures following best practices and relevant NIST-800- 53r4 controls from the CM family, which requires an annual review and update (as well as spontaneous review when critical changes is needed).</p> | |

| # | Question | Response |
|-----|---|--|
| 5.2 | <p>Does your organization track, review, approve or disapprove, and log changes to organizational information systems?</p> <p>(ARS v3.1 CM-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We leverage Confluence (https://www.atlassian.com/software/confluence) to document baseline configuration, and Jira ticketing system (https://www.atlassian.com/software/jira) and/or github issue on private repo to document initial change proposal, review process, as well as approval or disapproval decisions made by Role-B and Key Stakeholders. For approved changes, we will implement it using CloudFormation (https://aws.amazon.com/cloudformation/) , CodeCommit (https://aws.amazon.com/codecommit/) and CodePipeline (https://aws.amazon.com/codepipeline/) to effectively manage all AWS resources and accounts throughout their lifecycle by treating infrastructure as code following the best practice of version control. All the tools we used for change control management have built-in version control that tracks historical changes for as long as needed.</p> | |
| 5.3 | <p>Does your organization establish and enforce security configuration settings for information technology products employed in the organizational information systems?</p> <p>(ARS v3.1 CM-06)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We leverage the following three sets of complementary security policy packages:</p> <ol style="list-style-type: none"> 1. Control Tower mandatory and recommended Guardrails (https://docs.aws.amazon.com/controltower/latest/userguide/guardrails.html) 2. The AWS Foundational Security Best Practices standard (https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html) and CIS AWS Foundations Benchmark standard (https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-cis.html) deployed in GuardDuty (https://aws.amazon.com/guardduty/), with findings sent to SecurityHub (https://aws.amazon.com/security-hub/); 3. NIST-800-53r4 conformance pack (https://github.com/aws-labs/aws-config-rules/blob/master/aws-config-conformance-packs/Operational-Best-Practices-for-NIST-800-53-rev-4.yaml) . <p>We also have deployed AWS Config and AWS System Manager to continuously monitor and record our AWS resource configurations and automate the evaluation of recorded configurations against desired configurations.</p> | |

5B. Configuration Management Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 5.4 | <p>Does your organization ensure that there is a current baseline configuration image for hosts within the information system?</p> <p>(ARS v3.1 CM-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>Click here to enter text (<i>Optional</i>).</p> | |

| # | Question | Response |
|-----|---|--|
| 5.5 | Does your organization ensure that the information system uses physical and logical access restrictions to prevent unauthorized changes to the information systems? (ARS v3.1 CM-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 5.6 | Does your organization ensure that configuration of the information systems allows only essential functions, software, ports, protocols, and applications? (ARS v3.1 CM-07) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 5.7 | Does your organization maintain an up-to-date system inventory of Metadata to include all boundary components, such as: Each component's unique identifier and/or serial number; the information system of which the component is a part; the type of information system component (e.g., server, desktop, application); the manufacturer/model information; the operating system type and version/service pack level; the presence of virtual machines; the application software version/license information; the physical location (e.g., building/room number); the logical location (e.g., IP address, position with the information system [IS] architecture); the media access control (MAC) address; ownership; operational status; primary and secondary administrators; and primary use? (ARS v3.1 CM-08, CM-08(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 5.8 | Does your organization ensure that the information system prevents users from installing non-approved software through user policies? (ARS v3.1 CM-11) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

6A. Contingency Planning Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 6.1 | Does your organization have a policy for contingency planning that is reviewed/updated at least once a year? (ARS v3.1 CP-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have developed a full suite of policy and procedures following best practices and relevant NIST-800- 53r4 controls from the CP family which is required to be renewed/updated on an annual basis (as well as spontaneous review when critical changes is needed). | |
| 6.2 | Does your organization perform full weekly and incremental daily backups of user-level information, system-level information, and information system documentation including security-related documentation backups? How does your organization protect the confidentiality, integrity, and availability of backup information at the storage locations? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|---|--|----------|
| | (ARS v3.1 CP-09) | |
| | <p>We leverage AWS Backup service to centralize and automate the backing up of data across AWS services and create policies or “backup plans” to backup user-level information and system-level information on weekly basis. Information system documentation including security-related documentation are stored and backed up within Confluence and secure OneDrive with restricted access control. Data in S3 buckets are stored in three or more Availability Zones by default and we always enable “Object Versioning” (https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html) , which stores every different version of each object to prevent accidental overwriting.</p> | |

6B. Contingency Planning Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to 7A.

7A. Identification and Authentication Controls: Attestation and Rationale

| # | Question | Response |
|-----|---|--|
| 7.1 | Does your organization have a policy for identification and authentication that is reviewed/updated at least once a year? (ARS v3.1 IA-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We have developed a full suite of policy and procedures following best practices and relevant NIST-800- 53r4 controls from the IA family which is required to be renewed/updated on an annual basis (as well as spontaneous review when critical changes is needed).</p> | |
| 7.2 | Does your organization authenticate the identities of users, processes, or devices prior to granting access to organizational systems? Describe how your organization establishes initial content for authenticators; defines reuse conditions; and sets minimum and maximum lifetimes for each authenticator type to be used. (ARS v3.1 IA-02, IA-03, IA-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>As described in AC-2, we follow a rigorous governance process to evaluate users before granting them accesses to this cloud-based information system, which requires that all research personnel are linked to specific projects during the Institutional Review Board (IRB) review procedures. Updates are conducted at least annually, though the PI and other key stakeholders are expected to notify the IRB when there are staffing changes in the interim period. No research project begins without an HSC approval or valid CITI Human Subject Research certificate. The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. The passwords for the user accounts will have a maximum lifetime of 60 days. The passwords cannot be reused for a minimum of 12 cycles and have to meet the requirements for strength. The passwords have to be a minimum of 15 characters and should contain at least one number, one special character and one upper case letter. Management console is automatically logged-off every 12 hours. Inactive users will be disabled after 60 Data Management Plan Self-Attestation Questionnaire (DMP SAQ) November 12, 2020 Data Privacy Safeguard Program (DPSP) Page 14 # Question</p> | |

| # | Question | Response |
|---|---|----------|
| | Response days of inactivity. We manage access to all resources in the AWS Cloud by ensuring MFA is enabled for the root user and IAM users. | |

7B. Identification and Authentication Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 7.3 | Does your organization's information system use unique identifiers for users and scheduled processes (e.g., backups)? (ARS v3.1 IA-02) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 7.4 | Does your organization ensure the information system uniquely identifies devices (e.g., IP address, hostname, etc.)? (ARS v3.1 IA-03) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 7.5 | Does your organization successfully assign unique identifiers to users and devices; prevent reuse of identifiers for three (3) years; and disable identifiers after 60 days of inactivity? (ARS v3.1 IA-04) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 7.6 | Does your organization ensure the information system shows non-descript information when authentication fails? (ARS v.3.1 IA-06) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

8A. Incident Response Controls: Attestation and Rationale

| # | Question | Response |
|-----|--|--|
| 8.1 | Does your organization have an incident response policy that is reviewed/updated at least once a year? (ARS v3.1 IR-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have developed a full suite of policy and procedures following best practices and relevant NIST-800- 53r4 controls from the IR family, which is required to be renewed/updated on an annual basis (as well as spontaneous review when critical changes is needed) | |
| 8.2 | How does your organization investigate (e.g., preparation, detection, analysis, containment, eradication, and recovery) and track security incidents (e.g. physical, technical, and privacy)? (ARS v3.1 IR-04, IR-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|---|--|----------|
| | <p>Per the terms of the Data Use Agreement, the user will be responsible for reporting to CMS any breach in the security or primary of CMS data. The MU Mandator Reporting Requirement (https://www.umsystem.edu/ums/is/infosec/hr-mandatory-reporting) is generalizable to incidents response with respect to the CMS data files. Following excerpts from the policy define the responsibilities of MU staff when reacting and/or responding to the various types of network and information security incidents that may occur:</p> <ol style="list-style-type: none"> 1. All information security incidents and suspected incidents must be immediately reported to the appropriate central information security office at your campus or business entity. 2. All information security weaknesses must be immediately reported to your departmental IT office or central IT office. 3. All University faculty, staff and student employees must comply with this requirement. Failure to report information security incidents, suspected incidents or known weaknesses may result in disciplinary action. 4. All University faculty, staff and student employees are strongly encouraged to report any other conditions or circumstances that, if addressed, would improve the overall security environment. 5. Notify the MU Health Information Security Officer and MU Health System Privacy Officer of potential exposure of ePHI if the account has been proven to be accessed by unauthorized individuals. <p>As an enhancement to the existing organizational policy, we will acknowledge CMS DUA policy that requires CMS be notified of any potential incidents within 1 hour of discovery. The key stakeholders (i.e., PI or PI designee) will be responsible for reporting to CMS of any potential incidents. In addition, per our Corporate Compliance (https://www.muhealth.org/about-us/corporate-compliance) and Code of Conduct, any breach includes any inappropriate or unauthorized use, access or disclosure of PHI. If you observe or are aware of a breach of PHI, report it immediately to your supervisor, manager, department head, appropriate school leadership, MU Health System Privacy Officer (compliance@health.missouri.edu, (573) 884-0632), Human Resources, or the Hotline (Integrity and Accountability Hotline at (866) 447-9821). Furthermore, we required system users to report in writing to the MU Central Information Security Officers (secure.umsystem-accountability.ethicspoint.com) any use or disclosure of protected health information covered by the Agreement that becomes known to system user, within 24 hours of its discovery.</p> | |

8B. Incident Response Controls: Attestation

| # | Question | Response |
|-----|---|--|
| 8.3 | <p>Does your organization ensure that employees whom have incident response duties complete incident response training within one (1) month of assuming the role and complete/update incident response training at least once a year?</p> <p>(ARS v3.1 IR-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 8.4 | <p>Does your organization have the capability to investigate security incidents, that includes preparation, detection, analysis, containment, eradication, and recovery?</p> <p>(ARS v3.1 IR-04, IR-05)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|-----|--|--|
| | Click here to enter text (<i>Optional</i>). | |
| 8.5 | Does your organization investigate (e.g., preparation, detection, analysis, containment, eradication, and recovery) and track security incidents (e.g., physical, technical, and privacy)? (ARS v3.1 IR-04, IR-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 8.6 | Does your organization have incident response resources that can assist system administrators (e.g., help desks, assistance groups, access to forensics services, etc.)? (ARS v3.1 IR-07) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 8.7 | Does your organization's information system have an incident response plan that provides: The organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; reviewed and approved by the applicable Incident Response Team Leader; distributes copies of the incident response plan to the organization's information security officers and other incident response team personnel; review the incident response plan within every 365 days; update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; communicate incident response plan changes to the organizational elements listed above; and protects the incident response plan from unauthorized disclosure and modification? (ARS v3.1 IR-08) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

9A. Maintenance Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 9B.

9B. Maintenance Controls: Attestation

| # | Question | Response |
|-----|--|--|
| 9.1 | Does your organization have a system maintenance policy that is reviewed/updated at least once a year? (ARS v3.1 MA-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

| # | Question | Response |
|-----|--|--|
| 9.2 | Does your organization ensure it is not utilizing diagnostic hardware, software, or firmware maintenance tools that have been improperly modified within the data center? (ARS v3.1 MA-03, MA-03(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 9.3 | Does your organization check media containing diagnostic and test programs being introduced into the system for malicious code, where applicable? (ARS v3.1 MA-03(02)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

10A. Media Protection Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 10B.

10B. Media Protection Controls: Attestation

| # | Question | Response |
|------|---|--|
| 10.1 | Does your organization have a media protection policy that is reviewed/updated at least once a year? (ARS v3.1 MP-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.2 | Does your organization ensure the information system administrators mark system media based on the classification of information the media holds? (ARS v3.1 MP-03) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.3 | Does your organization protect and securely stores digital media and ensure it is overwritten once with a "00000000x" pattern or degaussed with a NIST approved degaussing device? (ARS v3.1 MP-04, MP-06) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.4 | Does your organization protect media: While being transported, to include hand-carried – uses a securable container (e.g., locked briefcase) via authorized personnel; shipped – tracks with receipt by commercial carrier; maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|------|--|--|
| | media; and restricts the activities associated with the transport of information system media to authorized personnel? (ARS v3.1 MP-05) | |
| | Click here to enter text (<i>Optional</i>). | |
| 10.5 | Does your organization sanitize media prior to disposal or reuse and track such activities? (ARS v3.1 MP-06, MP-06(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.6 | Does your organization prohibit the use of personally owned media? (ARS v3.1 MP-07, MP-07(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.7 | Does your organization ensure that any portable media devices have an identified owner? (ARS v3.1 MP 07, MP-07(01)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 10.8 | Does your organization ensure that records of disposed media which contain sensitive information are maintained? (ARS v3.1 MP-CMS-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

11A. Physical and Environmental Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 11B.

11B. Physical and Environmental Controls: Attestation

| # | Question | Response |
|------|--|--|
| 11.1 | Does your organization have a physical and environmental policy that is reviewed/updated at least once a year? (ARS v3.1 PE-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 11.2 | Does your organization maintain a current list of authorized individuals to enter the facility? (ARS v3.1 PE-02) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

| # | Question | Response |
|------|---|--|
| 11.3 | <p>Does your organization ensure it:</p> <p>Verifies individual access authorizations before granting access to the facility; controls ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan); maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan); provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible; escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); secures keys, combinations, and other physical access devices; inventories defined physical access devices (defined in the applicable security plan), no less often than every (90 High, 90 Moderate, or 180 Low) days; and changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated?</p> <p>(ARS v3.1 PE-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 11.4 | <p>Does your organization ensure that telephone and network hardware and transmission lines are protected?</p> <p>(ARS v3.1 PE-04)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 11.5 | <p>Does your organization ensure that all unused physical ports (e.g., wiring closets, patch panels, etc.) are physically or logically disabled, locked, or barred?</p> <p>(ARS v3.1 PE-04)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

12A. Planning Controls: Attestation and Rationale

| # | Question | Response |
|------|--|--|
| 12.1 | <p>Does your organization have a complete and up-to-date system security plan? How often is it reviewed/updated?</p> <p>(ARS v3.1 PL-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have developed a system security plan (SSP) comprising of a full suite of policy and procedures following best practices and relevant NIST-800-53r4 controls from all 19 control families, which is required to be renewed/updated on an annual basis. | |
| 12.2 | <p>Does your organization ensure that rules of behavior (e.g. user agreements, system use agreements, etc.) are signed by all users and administrators? Is this updated/reviewed at least once a year? How is it acknowledged?</p> <p>(ARS v3.1 PL-04)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| | |
|--|---|
| | <p>All system users are bound by the GPC Master Data Sharing Agreement (DSA, which outlined in Section 4.05 (“Data Use Agreement Among the Parties”) that the Parties shall comply with applicable laws and HIPAA regulations. The GPC Administrative Site and member institutions are bound by the PCORI Contract (“CDRN-1306-04631”), including Section X (“General Terms and Conditions”), which relates to confidentiality. All project staff are also bound by the GPC External Collaborator Agreement requiring External Institution to comply and ensure that its Affiliate Investigators comply with all applicable laws, rules and regulations, including the Privacy Rule and Security Rule. The External Institution and its Affiliate Investigators agree to use appropriate physical, technical, and administrative safeguards to prevent use or disclosure of the GPC Data other than as provided for by this Agreement. All users are also required to take annual training and provide signatures of acknowledgement upon completion. Training material (including a system-specific Standard Of Practice (SOP) that outlines relevant regulatory and operational policies regarding content, use, and access of the CMS data files) are reviewed and updated on an annual basis. Additionally, all relevant material (including data management plan and project staff list) are submitted as part of the Institutional Review Board (IRB) review and approval process at Data Custodian Organization, which is also required to be renewed on a yearly basis.</p> |
|--|---|

12B. Planning Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to 13B.

13A. Personnel Security Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 13B.

13B. Personnel Security Controls: Attestation

| # | Question | Response |
|------|--|--|
| 13.1 | <p>Does your organization follow CMS policy regarding background checks and screening for employees with access to CMS data?</p> <p>(ARS v3.1 PS-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 13.2 | <p>Does your organization ensure that employee termination follows the following steps:</p> <p>Disables information system access before or during termination; terminates/revokes any authenticators/credentials associated with the individual; conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; retrieves all security-related organizational information system-related property; retains access to organizational information and information systems formerly controlled by the terminated individual; notifies defined personnel or roles (defined in the applicable security plan) within one (1) calendar day; and immediately escorts employees terminated for cause out of the organization?</p> <p>(ARS v3.1 PS-04)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|------|---|--|
| | Click here to enter text (<i>Optional</i>). | |
| 13.3 | Does your organization have processes for re-screening personnel according to organizationally defined conditions as required? (ARS v3.1 PS-03) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 13.4 | Does your organization ensure that users sign access agreements every 365 days? (ARS v3.1 PS-06) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 13.5 | Does your organization ensure that third-party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees? (ARS v3.1 PS-07) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 13.6 | Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures? (ARS v3.1 PS-08) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

14A. Risk Assessment Controls: Attestation and Rationale

| # | Question | Response |
|------|--|--|
| 14.1 | Does your organization utilize an automated vulnerability scanner in compliance with organizational policies? How is this performed? (ARS v3.1 RA-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We will utilize AWS native vulnerability scanner, the AWS Inspector, and/or Qualys Agent to perform automated vulnerability scan in the information system and hosted applications at least every 72 hours. Scans for vulnerabilities in the information system and hosted applications are authenticated to the target system as a privileged user with a dedicated account (“Audit account”). “CRITICAL” and “HIGH” vulnerabilities are expected to be remediated immediately, while “MODERATE” and “LOW” vulnerabilities on a quarterly basis, in accordance with assessment results. Remediations will be handled manually based on built-in recommendations from AWS after consulting with Security Team, which will be converted to automated workflow when feasible.</p> | |

14B. Risk Assessment Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to 15B.

15A. System and Services Acquisition Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 15B.

15B. System and Services Acquisition Controls: Attestation

| # | Question | Response |
|------|--|--|
| 15.1 | Does your organization's administrators: Document configuration of the individual hosts within the system; how to perform maintenance of security functions; known vulnerabilities (can be tracked through a Plan of Action and Milestones (POA&M)); and other documentation as needed for use and operation of the system? (ARS v3.1 SA-05) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 15.2 | Does your organization ensure that the information system architecture is designed following security engineering principles (consistent with NIST SP 800-160 Volume 1)? (ARS v3.1 SA-08) | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 15.3 | Does your organization ensure that any external services (third-party ticketing, messaging, auditing, monitoring, etc.) outside of the accreditation/authorization boundary comply with organizational information security requirements? (ARS v3.1 SA-09) | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

16A. System and Communications Protection Controls: Attestation and Rationale

| # | Question | Response |
|------|--|--|
| 16.1 | Does your organization monitor, control, and protect communications (e.g., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems? What type of system is used? (ARS v3.1 SC-07) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Deploy services (such as Amazon Elastic Compute Cloud (Amazon EC2) instances, Lambda and etc.) within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely | |

| # | Question | Response |
|------|--|--|
| | within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. When restriction to VPC becomes infeasible (e.g. S3 bucket), we enforce rules such as “require SSL/TLS encryption or certification” and/or “require requests to use Secure Socket Layer (SSL)” and/or “No public IP allowed”. All network access points will be protected by a firewall and intrusion prevention systems that monitor and control communications. Traffic matching specific reconnaissance, intrusion or virus patterns will be prevented from entering or exiting the network. | |
| 16.2 | Does your organization ensure that the information systems use FIPS 140-2 validated cryptographic modules for transmission of data-in-motion and/or data-at-rest? (FIPS 140-2; ARS v3.1 SC-08, SC-13, SC-28) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | To ensure that data is encrypted properly using FIPS 140-2 validated cryptographic modules both in transit and at rest, we only allow the use adoption of AWS services with an FIPS endpoints (https://aws.amazon.com/compliance/fips/). We always require using SSL/TLS and following protocols SFTP and HTTPS when feasible. We also use AWS KMS service to further enforce encryption at rest (e.g., for data stored in S3 bucket) | |

16B. System and Communications Protection Controls: Attestation

| # | Question | Response |
|------|---|--|
| 16.3 | Does your organization ensure that administrative and regular user interfaces are separate? (ARS v3.1 SC-02) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 16.4 | Does your organization ensure the information system has the ability to terminate a network connection at the end of the session or after a defined period of inactivity? (ARS v3.1 SC-10) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 16.5 | Does your organization have a centralized cryptographic key management system that complies with organizational standards? (ARS v3.1 SC-12) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 16.6 | Does your organization prohibit collaborative computing mechanisms (e.g. networked white boards, cameras, microphones, etc.) unless explicitly authorized? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|---|---|----------|
| | (ARS v3.1 SC-15) | |
| | Click here to enter text (<i>Optional</i>). | |

17A. System and Information Integrity Controls: Attestation and Rationale

| # | Question | Response |
|------|---|--|
| 17.1 | <p>Does your organization update malicious code protection mechanisms when new releases are available and perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed?</p> <p>(ARS v3.1 SI-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>There are mainly two types of external sources expected to be interacted with the cloud-based information system that can only be performed by Role-B administrators: Data Management Plan Self-Attestation Questionnaire (DMP SAQ) November 12, 2020 Data Privacy Safeguard Program (DPSP) Page 24 # Question Response a) Inbound of research data from multiple secured and protected environment via secure transfer protocol. b) Installation of new software packages (e.g., Python, R) in a central private location, which can be shared with other Role-C users within their individual Integrated Development Environment centrally managed by Role-B.</p> <p>As described in RA-5, automated vulnerability scans are performed in the information system and hosted applications at least every 72 hours. All detective and preventive security guardrails and controls (described in CM-5) are checked by GuardDuty with findings sent to SecurityHub and alerts to CloudWatch on a daily basis.</p> | |
| 17.2 | <p>How does your organization monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks? Is the monitoring used to identify unauthorized use of organizational systems?</p> <p>(ARS v3.1 SI-04, SI-04(04))</p> | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>We will fully exploit the defense-in-depth architecture warranted by the AWS Well-Architected Framework (https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html) by leveraging the following managed services:</p> <ul style="list-style-type: none"> We enable Amazon GuardDuty to help monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. We also deploy AWS Security Hub to help monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. | |

| # | Question | Response |
|------|---|--|
| | <ul style="list-style-type: none"> Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. | |
| 17.3 | <p>Does your organization use file integrity monitoring (FIM), deploy tools and capabilities to monitor changes to critical resources such as operating system software components (e.g., OS images, kernel drivers, daemons), system firmware (e.g., the basic input/output system [BIOS]), and vital applications? (ARS v3.1 SI-07)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | <p>An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.</p> <p>We utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.</p> | |

17B. System and Information Integrity Controls: Attestation

| # | Question | Response |
|------|---|--|
| 17.4 | <p>Does your organization's information system: Identify system flaws; test updates prior to installation on production systems; correct high/critical security-related system flaws within ten (10) business days on production servers and 30 days on non-production servers; centrally manage flaw remediation; and track and approve any security-related patches which are not installed? (ARS v3.1 SI-02)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 17.5 | <p>Does your organization's information system use malicious code protection that has up-to-date virus definitions and scans important file systems every 12 hours and full system every 72 hours? (ARS v3.1 SI-03)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 17.6 | <p>Are email servers being hosted by the organization in the authorization boundary? Are spam filters used with the mail servers? (ARS v3.1 SI-08)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

| # | Question | Response |
|------|--|--|
| 17.7 | Does your organization's information system validate user input before accepting it into the system (e.g., sanitize user input within username and password fields)? (ARS v3.1 SI-10) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 17.8 | Does your organization ensure the information systems retains information in accordance with federal law, CMS policy, and HIPAA requirements? (ARS v3.1 SI-12) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

18A. Program Management Controls: Attestation and Rationale

| # | Question | Response s |
|------|--|--|
| 18.1 | Has your organization appointed and/or identified a senior information security officer with the authority to coordinate, develop, implement, and maintain an organization-wide information security program? (ARS v3.1 PM-02) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | We have ensembled an information security team ("Security Team") comprising of infosec personnel from University of Missouri system level (MU DoIT) and University of Missouri HealthCare Division level (MUHC Infosec), led by chief information security officer at MU. The Security Team is closely engaged throughout the policy and procedures development phase as well as post-deployment phase to continuously monitor security control requirements with Role-B administrators. | |

18B. Program Management Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to the Section 5: Privacy Controls.

5. PRIVACY CONTROLS

19. Accountability, Audit and Risk Management

| # | Question | Response |
|------|---|--|
| 19.1 | Does your organization have an office or department responsible for overseeing data privacy, the monitoring of privacy laws and policies, and the development of a strategic organizational privacy plan? (ARS v3.1 AR-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|------|--|--|
| | Click here to enter text (<i>Optional</i>). | |
| 19.2 | Does your organization review a random sample of contracts for contractors and service providers every two (2) years that provides maintenance for a system of records; ensures that the contracts include Privacy Act compliance clauses; and has defined privacy roles, responsibilities, and access requirements? (ARS v3.1 AR-03) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 19.3 | Does your organization monitor privacy policies and audit privacy controls at least once every year? (ARS v3.1 AR-04) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 19.4 | Does your organization develop, implement, and routinely update a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures? (ARS v3.1 AR-05a) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 19.5 | Does your organization ensure that personnel (manually or electronically) accept responsibilities for privacy requirements, including their obligation to protect the confidentiality and integrity of data, at least once every year? (ARS v3.1 AR-05b, c) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 19.6 | Does your organization ensure that an accurate accounting of information disclosures is in each system of records to include: the date, nature, purpose of each record disclosure, and list the address of a person or agency to whom the disclosure was made, for the life of the record or five (5) years after the disclosure was made (whichever is longer), and available to the person named in record upon request? (ARS v3.1 AR-08) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |
| 19.7 | Does your organization have an accountability, audit, and risk management policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|---|---|----------|
| | (ARS v3.1 AR-CMS-01) | |
| | Click here to enter text (<i>Optional</i>). | |

20. Authority and Purpose

| # | Question | Response |
|------|---|--|
| 20.1 | Does your organization have an authority and purpose policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed? (ARS v3.1 AP-CMS-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

21. Data Minimization and Retention

| # | Question | Response |
|------|--|--|
| 21.1 | Does your organization ensure that the minimum personally identifiable information (PII) elements identified are relevant and necessary to accomplish collection and have express CMS authorization? (ARS v3.1 DM-CMS-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

22. Data Quality and Integrity

| # | Question | Response |
|------|---|--|
| 22.1 | Does your organization have a data quality and integrity policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed? (ARS v3.1 DI-CMS-01) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (<i>Optional</i>). | |

23. Individual Participation and Redress

| # | Question | Response |
|---|----------|----------|
|---|----------|----------|

| | | |
|---|---|--|
| 23.1 | <p>Does your organization have an individual participation and redress policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed?</p> <p>(ARS v3.1 IP-CMS-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>Click here to enter text (Optional).</p> | | |

24. Security

| # | Question | Response |
|---|--|--|
| 24.1 | <p>Does your organization have a security policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed?</p> <p>(ARS v3.1 SE-CMS-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>Click here to enter text (Optional).</p> | | |

25. Transparency

| # | Question | Response |
|---|--|--|
| 25.1 | <p>Does your organization have a transparency policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed?</p> <p>(ARS v3.1 TR-CMS-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>Click here to enter text (Optional).</p> | | |

26. Use Limitation

| # | Question | Response |
|---|--|--|
| 26.1 | <p>Does your organization have a use limitation policy that identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every two (2) years or as needed?</p> <p>(ARS v3.1 UL-CMS-01)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>Click here to enter text (Optional).</p> | | |
| 26.2 | <p>Does your organization use PII or PHI internally – only for authorized purpose(s) identified in the Privacy Act, and externally – only for authorized purposes by</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

| # | Question | Response |
|------|---|--|
| | <p>permission of an authorized business associate agreement with third parties, specifically describing the PII and the purpose for which it may be used?</p> <p>(ARS v3.1 UL-01, UL-02a, b)</p> | |
| | Click here to enter text (Optional). | |
| 26.3 | <p>Does your organization monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII as well as evaluate any proposed new instances of sharing PII with third parties?</p> <p>(ARS v3.1 UL-02c, d)</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| | Click here to enter text (Optional). | |

6. DATA CUSTODIAN ATTESTATION

- I acknowledge my appointment as Data Custodian on behalf of the requesting organization and agree to comply with the provisions of any Data Use Agreement (DUA) with CMS where I am listed as the Data Custodian.
- As the Data Custodian, it is my responsibility to monitor the DUAs that cover data stored in the environment listed in section 1 of this DMP SAQ.
- As the Data Custodian, it is my responsibility to monitor the data recipients who receive CMS data and load the data into the environment listed in section 1 of this DMP SAQ.
- All of the information provided in this DMP SAQ is accurate, true, and complete to the best of my knowledge.
- I must notify the Data Privacy Safeguard Program (DPSP) of any changes to the information provided in this Data Management Plan Self-Attestation Questionnaire (DMP SAQ) within fifteen (15) days at data_privacy_safeguard_program@mbtechnologies.com.
- I further understand that any false information may result in the denial or revocation of my organization's Data Use Agreements (DUAs).

Signature: _____

Date: _____

| FOR OFFICE USE ONLY | |
|-------------------------|--|
| DMP SAQ Approval Date | |
| DMP SAQ Expiration Date | |