MHDO Data Management Attestation Questionnaire

**PURPOSE:** The Maine Health Data Organization (MHDO) data contains sensitive information that requires evidence that adequate data security and privacy safeguards are in place to protect the confidentiality, integrity, and availability of MHDO data. The following questionnaire will support your request in attesting and demonstrating your compliance with MHDO data management requirements, specifically the MHDO requirements outlined in [MHDO Rule Chapter 120](https://mhdo.maine.gov/rules.htm) and the [MHDO Data Use Agreement (DUA).](https://mhdo.maine.gov/_dataRqstDocs/MHDO%20DUA%20V5.1%20220602.docx)

# 1. DATA APPLICANT AND DATA RECIPIENT INFORMATION

*The Data Applicant is the Individual/Organization requesting MHDO data for their stated project and purpose in the MHDO application. The Data Recipient is the Individual/Organization responsible for the storage of the MHDO data. Both the Applicant and Recipient are 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.* ***Note****: the data applicant and data recipient may be the same Individual/Organization.*

|  |  |
| --- | --- |
| **DATA APPLICANT NAME** |  |
| **DATA APPLICANT ORGANIZATION**  |  |
| **DATA RECIPIENT NAME** |  |
| **DATA RECIPIENT ORGANIZATION**  |  |
| **DATA RECIPIENT OFFICE ADDRESS** |  |
| **DATA RECIPIENT PHONE NUMBER** |  |
| **DATA RECIPIENT EMAIL ADDRESS** |  |
| **COMPUTING ENVIRONMENT TYPE**  | ☐ Cloud Service Provider (CSP) [ ]  Onsite (local hard drive or network drive) ☐ Hybrid: Uses CSP & Exists Onsite |

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

|  |  |
| --- | --- |
| **SECONDARY POC**  |  |
| **SECONDARY POC PHONE NUMBER**  |  |
| **SECONDARY POC EMAIL ADDRESS**  |  |

# 2. INSTRUCTIONS FOR COMPLETING THIS FORM

This form is derived from the CMS Data Privacy Safeguard Program, Data Management Plan Self-Attestation Questionnaire and contains data security and privacy controls based on the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* control reference structure.

**Security Controls:** 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.

**Privacy Controls:** The National Institute of Standards and Technology (NIST) defines 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.

**Rationale and policies:** If the answer is YES to any of the questions below, check the corresponding box and move on to the next question. If the answer is **NO,** check the corresponding box and please include a rationale in the textbox provided. A rationale should reference or describe how a control will be addressed by the Data Applicant and Data Recipient. Where applicable, reference specific organizational policies.

**Guidance:** For supplementary guidance on the MHDO data management requirements, refer to the MHDO requirements outlined in [MHDO Rule Chapter 120](https://mhdo.maine.gov/rules.htm) and the [MHDO Data Use Agreement (DUA).](https://mhdo.maine.gov/_dataRqstDocs/MHDO%20DUA%20V5.1%20220602.docx)

# 3. SECURITY & PRIVACY CONTROLS

1. **Security & Privacy Management**

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Responses**  |
| 1.1 | 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? | [ ]  Yes[ ]  No |
|  |
| 1.2 | 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? | [ ]  Yes[ ]  No |
|  |
| 1.3 | 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? | [ ]  Yes[ ]  No |
|  |
| 1.4 | Does your organization ensure that rules of behavior (e.g., user agreements, system use agreements, etc.) are signed by all users and administrators? | [ ]  Yes[ ]  No |
|  |
| 1.5 | 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 training on the terms and conditions of the [MHDO Data User Agreement](https://mhdo.maine.gov/_dataRqstDocs/MHDO%20DUA%20V5.1%20220602.docx)? 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?  | [ ]  Yes[ ]  No |
|  |
| 1.6 | 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?  | [ ]  Yes[ ]  No |
|  |

1. **System Access, Authentication & Security**

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Response**  |
| 2.1 | Does your organization authenticate the identities of users, processes, or devices prior to granting access to organizational systems?  | [ ]  Yes [ ]  No |
|  |
| 2.2  | Does your organization use logical access controls (e.g., roles, groups, file permissions) to restrict access to MHDO data to authorized users by requiring computer log-on with unique user accounts and passwords and multi-factor authentication?  | [ ]  Yes[ ]  No |
|  |
| 2.3 | Does your organization have the ability to segregate MHDO data from other institutional data? | [ ]  Yes [ ]  No |
|  |
| 2.4 | Does your organization have a process for approved information-sharing circumstances that determines what is shared with authorized external users (e.g., collaborators) and ensures that access authorizations assigned to these users aligns with the organization’s access restrictions?  | [ ]  Yes[ ]  No |
|  |
| 2.5 | Does your organization ensure that MHDO data-in-motion (data transmission) meet the minimum TLS protocol level of TLS1.2 and data-at-rest (data storage) will be encrypted with a key length of at least 256 bits?  | [ ]  Yes[ ]  No |
|  |
| 2.6 | Does your organization ensure that any device which contains MHDO data stored on a local hard drive, when not in use, will be physically secured so that access is restricted to authorized personnel (i.e., locked in an authorized user’s office)? | [ ]  Yes[ ]  No |
|  |
| 2.7 | For data stored using a Cloud Service Provider (CSP), a computing environment where your organization is not solely responsible for the implementation of data security requirements: Does your organization have evidence that the proposed computing environment (CSP) meets or exceeds NIST 800-53v4 security standards at the moderate control level? Examples of acceptable evidence for demonstrating NIST 800-53 compliance include:* Certification audit against ISO 27001
* Assessment and audit against HIPAA standards
* SSAE 16 Overview
* Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
* FedRAMP Certification

If your organization does not utilize a CSP, please select N/A. | [ ]  Yes [ ]  No[ ]  N/A |
|  |
| 2.8 | Does your organization ensure the information systems retains information in accordance with HIPAA requirements? | [ ]  Yes [ ]  No |
|  |

**3. Personnel Security**

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Response**  |
| 3.1  | Does your organization ensure that employee termination follows the following steps: * 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
 | [ ]  Yes[ ]  No |
|  |
| 3.2  | Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures?  | [ ]  Yes[ ]  No |
|  |
| 3.3 | 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?  | [ ]  Yes[ ]  No |
|  |

## 4. Data Quality and Integrity

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Response**  |
| 4.1  | 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?  | [ ]  Yes[ ]  No |
|  |

## 5. Media Protection & Data Destruction

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Response**  |
| 5.1  | Does your organization protect media: * While being transported, to include hand-carried – uses a securable container (e.g., locked briefcase) via authorized personnel.
* Maintains accountability for information system media during transport outside of controlled areas.
* Documents activities associated with the transport of information system media.
* Restricts the activities associated with the transport of information system media to authorized personnel.
 | [ ]  Yes[ ]  No |
|  |
| 5.2 | Does your organization follow NIST Special Publications 800-88, Guidelines for Media Sanitization, Revision 1? <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf> | [ ]  Yes[ ]  No |
|  |
| 5.3  | Does your organization ensure that records of disposed media which contain sensitive information are maintained?  | [ ]  Yes [ ]  No |
|  |

## 6. Incidence Monitoring, Response & Auditing

|  |  |  |
| --- | --- | --- |
| **#**  | **Question**  | **Response**  |
| 6.1 | 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?  | [ ]  Yes [ ]  No |
|  |
| 6.2 | Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation, and ongoing security assessments? | [ ]  Yes [ ]  No |
|  |
| 6.3 | Does your organization investigate (e.g., preparation, detection, analysis, containment, eradication, and recovery) and track security incidents (e.g., physical, technical, and privacy)?  | [ ]  Yes [ ]  No |
|  |
| 6.4 | Does your organization have the capability to audit events on the information system? Including: * User logon and logoff (successful and unsuccessful)
* All system administration activities
* Application alerts and error messages
* Audit logging service configuration changes
 | [ ]  Yes [ ]  No |
|  |
|  6.5 | 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? Including: * Date and time of the event (e.g., a timestamp)
* User or account that initiated the event (unique username/identifier)
* Event type
* Event outcome (succeed/failure)
* Any privileged system functions executed
 | [ ]  Yes [ ]  No |
|  |  |
| 6.6  | Does your organization ensure audit records are searchable and retained for at least one (1) year in archive storage?  | [ ]  Yes [ ]  No |
|  |

# 4. DATA APPLICANT AND DATA RECIPIENT ATTESTATION

1. I acknowledge my responsibility as Data Applicant on behalf of the requesting organization and agree to comply with the provisions of the MHDO Data Use Agreement.
2. I acknowledge my responsibility as Data Recipient on behalf of the requesting organization and agree to comply with the provisions of the MHDO Data Use Agreement.
3. All the information provided in this form is accurate, true, and complete to the best of my knowledge.
4. I will notify the MHDO of any changes to the information provided in this Data Management Attestation Questionnaire (DMAQ) within fifteen (15) days of the changes, by submitting an updated DMAQ and a letter identifying the section(s) of this form that have changed through the Data Request Portal.
5. I further understand that any false information or failure to make appropriate notifications to MHDO will result in the denial or revocation of my organization’s access to MHDO data.

**Data Applicant Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Data Recipient Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_