MDH POLICY

https://health.maryland.gov/Pages/mdhpolicies.asp

OFFICE OF THE SECRETARY -
01.06.01THE DATA OFFICE - STRATEGIC DATA INITIATIVE

MDH POLICY
Version Effective: 11/2/2022

MDH DATA USE POLICY

I. EXECUTIVE SUMMARY

The Maryland Department of Health (MDH) has the mission to promote and improve the health and safety of all Marylanders through disease prevention, access to care, quality management, and community engagement. MDH, through its mission, creates, receives, and stores large amounts of Data. MDH bears a responsibility to the public to provide stewardship and protections of sensitive Data.

This policy describes how MDH will control and regulate access to its electronic Data and systems. This policy provides a framework for review of all Data-Related Agreements involving the use of MDH Data by Data Partners and Trusted Data Partners.

II. BACKGROUND

In a series of Executive Orders, the State of Maryland prioritized Data security and privacy in all state agencies. These orders set forth specific requirements such as the establishment of a Data Office within MDH (01.01.2021.09). MDH is required to establish certain privacy practices by January 1, 2022 (01.01.2021.10). The orders also set forth requirements for Data-sharing among agencies through MDTHINK (01.01.2021.11). In response to these orders, MDH established the Strategic Data Initiative (SDI) Team to establish policies and guidance for MDH relating to Data control and usage and review of Data-Related Agreements involving Data controls and usage. In addition to this policy, all MDH employees shall follow the State of Maryland Information Security Manual (Version 1.2) which controls the Information Technology policies of all state agencies in Maryland.

This version supersedes the prior version of MDH Policy 01.06.01 dated June 13, 2022 and the prior version dated December 15, 2021. This November 2, 2022 version modifies language to “Trusted Data Partner” and establishes certain criteria for this designation. This version also adds a Data Governance Council as an independent subcommittee of the Strategic Data Initiative (SDI) Team focused on data governance and strategic oversight. This version also incorporates the name change of the Office of Internal Controls, Audit Compliance & Information Security (IAC/S) and incorporates the representative of IAC/S Office of Compliance and Privacy as a voting member of the SDI Team. This version also adds information regarding MDH Policy 01.06.02 MDH Information Technology Project & Fiscal Management Policy.

III. POLICY STATEMENTS

A. Definitions.

In this policy, the following terms have the meanings indicated.

1. **"Approval"** means the written notification by the SDI Team that indicates the submitted Data-Related Agreement has Appropriate Safeguards and Access Controls.

2. **"Approved System"** means those systems identified and maintained by the SDI Team in the Approved Systems list.

3. **"Appropriate Safeguards and Access Controls"** means security protections that are consistent with United States Department of Health and Human Services (HHS), Centers for Medicare and Medicaid Services (CMS), Maryland Department of InformationTechnology (DoIT), and MDH IT Security policies and standards.

4. **"Business Associate Agreement (BAA)"** means an agreement between a covered entity (MDH) and a business associate as defined in the HIPAA Privacy Rule. The elements of a BAA are outlined in the federal regulation at 45 CFR §164.504(e). A BAA is considered a Data-Related Agreement.

5. **"Data"** means any information stored electronically regardless of format.

6. **"Data Management"** means the development, execution, and supervision of policies, standards, and processes of all knowledge areas of data governance including: data architecture, data modeling and design, data storage and operations, data security, data integration and interoperability, documents and content management, reference and master data, data warehousing and business intelligence, metadata, and data quality.

7. **"Data Partner"** means any non-MDH individual or entity that is a party to an MDH Data-Related Agreement.

8. **"Data-Related Agreement"**

a. "Data-Related Agreement" means any and all agreements entered into by an MDH unit that involves the use or access of MDH Data.

b. "Data-Related Agreement" includes but is not limited to Business Associate Agreement, Data Use Agreement, and Memorandum of Understanding.

9. **"Data Use"** means the access, storage, transfer, and/or transformation of data through contribution, consumption, or computation.

10. **"MDH Data"** means Data that is created, received, stored, shared, or distributed by MDH or any of its units, regardless of the original source of the Data, for which MDH or any of its units:

a. Have a direct or indirect responsibility for security or privacy as a result of an agreement, contract, federal or State statute or regulation;

b. Have an implied or explicit duty of care; or

c. Can exercise control over the Data by:

i. Granting or restricting access; or

ii. Modifying or deleting the Data.

11. **"Personally Identifiable Information (PII)"** means any information about an individual that is managed, stored, or collected by an MDH unit, including:

a. Any information that can be used to distinguish or trace an individual's identity, including, but not limited to, Social Security number, date or place of birth, mother's maiden name, or biometric records; and

b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

12. **"Protected Health Information (PHI)"** means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, as defined by the HIPAA regulations, 45 CFR § 160.103.

13. **"Provisional Approval"** means the written notification by the SDI Team that indicates the submitted Data-Related Agreement presents a low or medium risk to MDH Data and information security based upon internal review of current data and security safeguards and access controls. Provisional approval shall include a determination memo with risk remediation recommendations from the SDI Team that must be completed within one year.

14. **"SDI Team"** means the group within MDH that reviews all Data-Related Agreements prior to implementation and includes the MDH Data Officer, MDH Chief Information Security Officer, a representative from the IAC/S Office of Compliance and Privacy, and a representative from the Office of Contract Management & Procurement (OCMP), or their designee(s). The Director of IAC/S is the Chair of the team and does not serve as a voting member. The MDH Chief Technology Officer, the MDH Chief Information Officer, and a representative from the Office of the Attorney General serve on the SDI Team in an advisory capacity.

15. **"Secretary"** means the Secretary of the Maryland Department of Health.

16. **"Trusted Data Partner"**

a. "Trusted Data Partner" is an entity that is:

i. A State agency or designee for a data role defined in statute, regulation, or executive order;

ii. An entity with a legacy data function that would have a critical business impact due to the difficulty of migration to a new entity; or

iii. An entity with data lake capability with bi-directional connectivity with the MDH data lake with periodic backups to MDH that support critical MDH business processes.

b. A "Trusted Data Partner" must:

i. Meet certain minimum-security standards as defined by the SDI Team;

ii. Meet certain data governance and management standards as defined by the SDI Team; and

iii. Be approved as a Trusted Data Partner by the SDI Team and the MDH Secretary.

B. General Policy.

Data Partners and Trusted Data Partners may use, view, or access MDH Data but must view, analyze, and create/store the Data exclusively in an Approved System, including, but not limited to, MDTHINK, Department of Information Technology (DoIT), and other MDH systems.

1. Prohibitions.

No MDH unit may enter into a Data-Related Agreement without prior approval from the SDI Team. MDH Data may not be used, accessed, or stored on any system that is not a State Approved System unless the MDH unit has been granted a waiver from the Secretary.

2. SDI Review Required.

The SDI Team shall review a Data-Related Agreement prior to its execution. Existing Data-Related Agreements executed prior to December 15, 2021, are subject to SDI Team review upon renewal of the agreement. Data-Related Agreements which cannot meet the standards requiring data use through a State Approved System, as outlined in this policy, must receive a waiver from the SDI Team and the Secretary prior to the use, access, or disclosure of MDH Data. The SDI Team may recommend exclusions from the policy to the Secretary as appropriate.

3. Applicability.

This policy applies to all Data-Related Agreements executed, extended, modified, or renewed on or after December 15, 2021. When a Data-Related Agreement is required by statute, regulation, law, or by terms of a grant, the MDH unit must still submit the Data-Related Agreement to the SDI Team via Cognito Forms. Further, for Data-Related Agreements with Trusted Data Partners, MDH units must still submit the agreement to the SDI Team via Cognito Forms. For Data-Related Agreements required by statute, regulation, law, or grants, the SDI Team will serve in an advisory capacity and provide

non-binding recommendations regarding the proposed Data-Related Agreement to the submitting MDH unit. For Data-Related Agreements with Trusted Data Partners, the SDI Team will conduct an expedited review process.

4. Review and Determination.

The SDI Team shall review all Data-Related Agreements submitted for review by MDH units via the Cognito Forms Platform. For a sample version of the form, please see Attachment 1: Strategic Data Initiative Agreement Review. The submission via Cognito Forms must include all relevant proposed contracts and documentation related to the Data-Related Agreement. Review by the SDI Team can result in the following outcomes: approval, provisional approval, recommendation for waiver from the Secretary, remand for additional information or correction, or denial. MDH units must comply with requests for additional information or correction from the SDI Team. Failure to do so within 30 days will require a resubmission to the SDI Team. For further information regarding the SDI Team's procedure, please see Attachment 2: SDI Team Standard Operating Procedure.

5. Designation as a Trusted Data Partner.

The SDI Team at their discretion can assess a data partner to determine if the data partner meets the criteria of a Trusted Data Partner. The SDI Team will initiate the Trusted Data Partner certification process on a case-by-case basis. If the SDI Team determines that the entity meets the requirement of a Trusted Data Partner, the SDI Team will send the recommendation to the Secretary for final approval.

C. Data Governance Council (DGC)

There is a Data Governance Council within the SDI Team. The DGC is responsible for strategic oversight and review of MDH data management efforts. The DGC is an independent sub-committee of the SDI Team. The DGC shall develop a standard operating procedure.

1. DGC Membership.

Principal members of the DGC include the following:

- MDH Data Officer;
- The Deputy Secretary for Public Health Services or their designee;
- The Deputy Secretary for the Behavioral Health Administration or their designee;
- The Deputy Secretary for Health Care Financing and Medicaid or their designee;
- The Deputy Secretary for Operations or their designee; and
- The Deputy Secretary for the Developmental Disabilities Administration or their designee.

Advisory members of the DGC may include the following:

- Data Governance Director, MDH Data Office;
- A representative from the Office of Enterprise Technology (either the Chief Information Officer or the Chief Technology Officer);
- A representative from the IAC/S focused on compliance and privacy;
- A representative from the IAC/S focused on information security; and

- Additional representatives from the MDH Data Office as appropriate.

The MDH Data Officer serves as the chair of the DGC. The chair may invite additional subject matter experts to the DGC meetings at their discretion. For further information on the DGC structure, please refer to Attachment 4: DGC Organizational Chart.

2. DGC Purpose.

The DGC shall focus on the development, implementation, management and enforcement of MDH data governance. The DGC may propose guidelines and policy recommendations to be approved by the MDH Data Office, SDI Team, and the MDH Secretary as appropriate. The DGC shall implement data governance best practices as outlined in the Data Management Body of Knowledge and Executive Order 01.01.2021.10.

D. Additional Data Use Considerations.

The hosting of MDH Data on State Approved Systems is one of many considerations for Data-Related Agreements. In addition to the MDH Data Use Policy, Data-Related Agreements are required to adhere to applicable federal or State statutes, regulations, and policies which may include but are not limited to:

1. Health Insurance Portability and Accountability Act (HIPAA).

Data that uses Protected Health Information (PHI) shall meet all requirements as outline in MDH HIPAA policies. Relevant policies include: HIPAA Individual Rights (01.03.05), HIPAA Privacy Administration Requirements (01.03.06), HIPAA Breach Response Policy (01.03.07), and Computerized Personal Information Breach Response (01.03.08).

2. Research Involving Human Subjects.

Data related to MDH research involving human subjects shall meet all requirements as outlined in the Policy on Research Involving Human Subjects and the MDH Institutional Review Board (IRB) (01.03.02).

3. Information Assurance.

MDH Data is also subject to the Policy to Assure Confidentiality, Integrity, and Availability of DHMH Information (02.01.06).

4. Information Technology Projects.

Effective August 3, 2022, MDH Policy 01.06.02 Information Technology Project and Fiscal Management Policy was issued. Prior to SDI Team review and approval of any Data-Related Agreement for an IT project, the IT project must have been reviewed and approved by the IT Executive Operations Committee as outlined in the policy.

IV. COMPLIANCE AND ENFORCEMENT

Any MDH unit or individual acting on behalf of an MDH unit that enters into a Data-Related Agreement after the effective date of this policy without approval by the SDI Team is subject to internal compliance reviews and appropriate disciplinary measures. The SDI Team, at their discretion, may recommend

appropriate enforcement measures and refer cases to the Secretary, the Office of Internal Controls, Audit Compliance & Information Security (IAC/S), or the Office of Human Resources as appropriate for Data-Related Agreements that do not follow this policy.

In the event of a data breach, MDH units must follow the existing MDH policies: HIPAA Breach Response Policy (01.03.07) and the Computerized Personal Information Breach Response Policy (01.03.08).

Further, MDH units must follow State Data and security policies, including but not limited to the State of Maryland Information Security Manual (Version 1.2).

V. ROLES & RESPONSIBILITIES

A. Office of the Attorney General (OAG).

The OAG provides legal review and assistance regarding Data-Related Agreements when requested by the SDI Team, the MDH unit that is a party to the Agreement under review, or the Secretary. OAG provides a representative to the SDI Team that serves as an advisory member.

B. Data Governance Council (DGC)

The Data Governance Council (DGC) is responsible for strategic oversight and review of MDH data management efforts. The DGC is an independent sub-committee of the SDI Team. The DGC will focus on the development, implementation, management, and enforcement of MDH data governance standards and policies. Principal members of the DGC include the MDH Data Officer, the Deputy Secretary for Public Health Services or their designee, the Deputy Secretary for the Behavioral Health Administration, the Deputy Secretary for Health Care Financing and Medicaid or their designee, the Deputy Secretary for Operations or their designee, and the Deputy Secretary for the Developmental Disabilities Administration or their designee. For further information on the DGC organizational structure, please refer to Attachment 4: DGC Organizational Chart.

C. MDH Chief Compliance Officer.

The MDH Chief Compliance Officer reviews Data-Related Agreements as an advisory member of the SDI Team.

D. MDH Chief Information Security Officer (CISO).

The MDH CISO reviews Data-Related Agreements to determine conformance to applicable information security best practices, standards, policies, regulations, and laws. The MDH CISO serves as a voting member of the SDI Team.

E. MDH Chief Technology Officer.

The MDH CTO reviews Data-Related Agreements as an advisory member of the SDI Team to determine conformance to applicable IT operational and architecture best practices, standards, policies, regulations, and laws.

F. MDH Chief Information Officer.

The MDH Chief Information Officer (CIO) reviews Data-Related Agreements as an advisory

member of the SDI Team to determine conformance to applicable IT operational and architecture best practices, standards, policies, regulations, and laws.

G. MDH Data Office.

The MDH Data Office reviews Data-Related Agreements to determine compliance with applicable Data governance best practices, standards, policies, regulations, and laws. The MDH Data Office provides technical support to the SDI Team as appropriate.

H. MDH Data Officer.

The MDH Data Officer serves as a voting member of the SDI Team reviewing Data-Related Agreements for compliance with applicable data governance best practices, standards, policies, regulations, and laws.

I. MDH Secretary.

The Secretary must approve the individual designated by OCMP to serve on the SDI Team. Also, the MDH Secretary determines at their discretion whether to authorize exclusions or waivers from this policy. Further, the MDH Secretary must approve any proposed Trusted Data Partners.

J. Office of Contract Management and Procurement (OCMP).

MDH's Office of Contract Management and Procurement reviews and approves all agreements between MDH and other parties, including public universities, other state agencies, private third-party vendors through procurement, and non-profit entities through grants. These agreements often incorporate terms and conditions that govern data use. Further, OCMP must designate an individual to serve on the SDI Team as a voting member.

K. Office of Internal Controls, Audit Compliance & Information Security (IAC/S).

MDH's Office of Internal Controls, Audit Compliance & Information Security (IAC/S) ensures that all MDH units are compliant with legal, regulatory, and policy requirements. IAC/S also reviews Data-Related Agreements and policy to protect MDH Data. The Director of IAC/S will Chair the Strategic Data Initiative (SDI) Team.

L. Office of Internal Controls, Audit Compliance & Information Security – Office of Compliance and Privacy.

MDH's Office of Internal Controls, Audit Compliance & Information Security (IAC/S) Office of Compliance and Privacy ensures that all MDH Data transferred to, collected by, stored by, or shared to external parties is done so consistent with federal and State law including but not limited to the HIPAA Privacy Rule, 42 CFR Part 2, and PII as defined in 42 CFR. § 200.79. The representative from IAC/S Office of Compliance and Privacy also reviews Data-Related Agreements to ensure MDH is protected in the event of a breach. The MDH representative from IAC/S Office of Compliance and Privacy serves as a voting member of the SDI Team.

M. Strategic Data Initiative Team.

The Strategic Data Initiative (SDI) Team is led by the Director of the Office of Internal Controls, Audit Compliance & Information Security (IAC/S). Voting members include the representative

from IAC/S Office of Compliance and Privacy, MDH Data Officer, and MDH Chief Information and Security Officer. Further, a representative from the Office of Contract Management and Procurement (OCMP) shall be designated and approved by the MDH Secretary. For the SDI Team's organization, see Attachment 3: SDI Team Organizational Chart. The SDI Team has the primary responsibility of ensuring all Data-Related Agreements that permit use, collection, storage, or access of MDH Data abide by policies and guidelines for data use as set forth in this policy. The SDI Team shall review all Data-Related Agreements for consistency with MDH policy and to complete a risk assessment of proposed Data-Related Agreements. The SDI Team has the authority to deny approval for Data-Related Agreements that do not meet MDH Data standards. Further, the SDI Team shall maintain a list of Trusted Data Partners.

N. Units Submitting to SDI Team.

Each MDH unit assumes the responsibility for the accuracy and completeness of the information provided when submitting a Data-Related Agreement to the SDI Team. MDH units shall timely comply with requests for clarification or questions from the SDI Team. Further, MDH units must respond to a remand for additional information or correction within 30 days; failure to do so will require a resubmission to the SDI Team.

VI. REFERENCES

- DAMA-DMBOK: Data Management Body of Knowledge, 2nd Edition Henderson, D., Earley, S, & Sebastian-Coleman, L. (Ed.) (2017). *Dama-Dmbok: Data Management Body of Knowledge* (2nd ed.). Technics Publications.

- Executive Order 01.01.2021.09 State Chief Data Officer:
  https://governor.maryland.gov/wp-content/uploads/2021/07/State-Chief-Data-Officer.pdf

- Executive Order 01.01.2021.10 Maryland Data Privacy:
  https://governor.maryland.gov/wp-content/uploads/2021/07/Maryand-Data-Privacy-EO.pdf

- Executive Order 01.01.2021.11 Maryland Total Human-services Integrated NetworK:
  https://governor.maryland.gov/wp-content/uploads/2021/07/Maryland-Total-Human-services-Integrated-NetworK.pdf

- Executive Order 01.01.2022.03 Maryland Total Human-services Integrated NetworK:
  https://governor.maryland.gov/wp-content/uploads/2022/04/Maryland-Total-Human-Services-Integrated-Network.pdf

- Maryland Department of Information Technology, State of Maryland Information TechnologySecurity Manual (Version 1.2):
  https://doit.maryland.gov/Documents/Maryland%20IT%20Security%20Manual%20v1.2.pdf
- MDH Policy to Assure Confidentiality, Integrity, and Availability of DHMH Information:
  https://health.maryland.gov/docs/02.01.06%20Information%20Assurance%20Policy%20-

- MDH Policy Computerized Personal Information Breach Response: https://health.maryland.gov/docs/01.03.08%20Computerized%20Personal%20Information%20Breach%20Response%20Policy%205-6-15.pdf
- MDH Policy HIPAA Breach Response: https://health.maryland.gov/docs/01.03.07%20HIPAA%20Breach%20Response%20Policy%207-22-14%20(1).pdf
- MDH Policy HIPAA Individual Rights: https://health.maryland.gov/docs/p010305.pdf
- MDH Policy HIPAA Privacy Administrative Requirements: https://health.maryland.gov/docs/p010306.pdf
- MDH Policy Information Technology Project and Fiscal Management Policy: https://health.maryland.gov/Documents/MDH%20Policy%2001.06.02%20-%20MDH%20Information%20Technology%20Project%20and%20Fiscal%20Management%20Policy.pdf
- MDH Policy on Research Involving Human Subjects Involving the MDH Institutional ReviewBoard (IRB): https://health.maryland.gov/docs/01.03.02%20IRB%20Policy%20-signed.pdf

VII. ATTACHMENTS

- Attachment 1: Strategic Data Initiative Agreement Review
- Attachment 2: Strategic Data Initiative Team Standard Operating Procedure
- Attachment 3: SDI Team Organizational Chart
- Attachment 4: DGC Organizational Chart

APPROVED:

Dennis R. Schrader, Secretary

November 2, 2022

Effective Date

Strategic Data Initiative Agreement Review

Please complete this form with the data partner (vendor) to request the Strategic Data Initiative (SDI) Team's review of your data-related agreement. Please direct any questions to mdh.sditeam@maryland.gov.

Note: Approval from the SDI Team or a waiver from the Secretary is required prior to signing any agreement allowing the use of MDH data with a potential data partner.

Updated 7/23 to include questions from the Data Survey. Submissions after 7/23 will no longer have to complete the Data Survey Google Form. Please complete this submission with the Data Partner (vendor).
Every answer must be filled out or the SDI Team will contact the unit for follow up.

What is the name of MDH unit requesting the review? *

What is the name of the MDH administration? *

What is the name of vendor or other party to the agreement? *

Is the vendor using a third-party IT provider? *

- ◯ Yes
- ◯ No

Is MDH Data shared or viewed by other partner vendors, sub-vendors, or partner organizations? *

- ◯ Yes
- ◯ No

Agreement or Project Title *

SDI #

For SDI Team use only

What type of agreement is proposed? *

- [ ] Business Associate Agreement
- [ ] Memorandum of Understanding
- [ ] Interagency Agreement
- [ ] Data Use Agreement
- [ ] Data Sharing Request Form
- [ ] Other

Check all that apply

Agreement Status *

- ( ) New
- ( ) Renewal
- ( ) Revision/Amendment
- ( ) Other

Note: Option renewals with no other modifications DO NOT require an SDI submission.

Is sharing of MDH data related to this agreement mandatory under a law, regulation, statute, or grant? *

( ) Yes ( ) No

Select the type:

- [ ] State or federal law
- [ ] Federal grant
- [ ] State grant
- [ ] Other grant
- [ ] Regulation
- [ ] Other

Check all that apply.

List the MDH data fields that are being viewed, used, shared, or stored by the other party/vendor. *

Name the specific datasets

For example: client referrals, patient name, birth records, race, ethnicity, Medicaid claims ID, number of clients referred, cases by zipcode. If no MDH datasets are involved, please explain.

What is the source of the MDH data? *

For example: LTSS Maryland, Vital Statistics, CRISP

What is the purpose for acquiring MDH Data? *

- [ ] Research
- [ ] Analysis
- [ ] Patient Records
- [ ] Patient Referral
- [ ] Acquiring Software or Services
- [ ] User Access to MDH Datasets
- [ ] Other

Check all that apply

Please check the types of MDH Data will be used for this agreement. *

- [ ] Aggregated/ Summary data
- [ ] Disaggregate Detail Level Data (non-PHI/PII)
- [ ] Personally Identifiable Information (PII)
- [ ] Protected Health Information (PHI)
- [ ] Federal Tax Information (FTI)
- [ ] Payment Card Industry (PCI) Data
- [ ] Other Confidential Data
- [ ] Other

PLEASE COMPLETE WITH VENDOR OR OTHER PARTY INPUT

Under this agreement, explain what tasks are being performed with the MDH data by the other party/vendor? *

Describe in detail what the other party will do with MDH data

How will the MDH Data be transmitted to the other party/vendor? *

List all methods of transmission, including sFTP, encrypted email (name the encryption method), State of Maryland Google Drive, analog fax, digital fax, etc.

How frequently will the MDH Data be transmitted? *

Approved Systems

- MDTHINK
- DoIT
- MDH Systems (Google Drive, Golden Image Laptops, Network Drive)

Where will the other party/vendor store the MDH data after transmission? *

- ◯ Currently on MD THINK
- ◯ Interested in using MD THINK for this agreement
- ◯ State Golden Image Laptop
- ◯ State of Maryland Google Drive
- ◯ Vendor or Third-Party Cloud System
- ◯ Other Vendor or Third-Party System
- ◯ Data is only being viewed
- ◯ Other

List any systems or applications the other party will use for collection, storage, management, and analysis of the MDH Data. *

Describe in detail where and how MDH Data will be stored by the other party

For example: OneDrive, encrypted email, encrypted laptops, MDH golden image laptops, secure fax, flash drives, hard copies, databases, Google/Microsoft drive, private data center, public cloud, business tools, etc.

Describe the access level to the MDH Data *

- [ ] Data is only being viewed
- [ ] Data will be downloaded to an MDH/State system
- [ ] Data will be downloaded to the other party/vendor's system
- [ ] There is no MDH Data being viewed, used, or shared.
- [ ] Other

Explain

If the other party is using laptops to download, store, or analyze the data, please select the type: *

Will MDH Data on the other party's system stay inside the US at all times? If no, explain. *

Are all the employees, vendors, sub-vendors, developers, and users accessing MDH Data physically located inside the US? If no, explain. *

Are all employees of the other party/vendor with access to PHI/PII MDH Data background-checked/drug-tested and provided HIPAA training? Explain. *

If no PHI/PII is involved, write N/A

What is the projected end date?

If no projected end date, explain.

If using a Third Party or Vendor, can the organization provide ONE of the following: *

- ◯ SOC-2 Report
- ◯ Risk Assessment Report
- ◯ HITRUST CERTIFICATION
- ◯ No
- ◯ Unknown
- ◯ Not applicable because MDH Data is not stored on another party's system

Attach a copy of the document in the "Upload" section.

Upload a copy of the proposed agreement and any other relevant documents. *

Upload or drag files here.

Note: Units must upload a copy of the pending agreement.

Name *

Name of person completing form.

Title *

Title of person completing form.

Email *

Email of person completing form.

Additional Emails (Optional)

Emails of individuals that should be copied on correspondence for this submission.

Submit

ATTACHMENT 2: Strategic Data Initiative Team Standard Operating Procedure

I. PURPOSE

The Strategic Data Initiative Team has the primary responsibility of ensuring all Data-Related Agreements that permit the use, collection, storage, or access of MDH Data abide by the policies and guidelines as set forth in the MDH Data Use Policy (01.06.01). The SDI Team shall review all Data-Related Agreements for consistency with the policy and complete a risk assessment of the proposed agreement.

II. MEMBERSHIP

The SDI Team consists of a representative from the IAC/S Office of Compliance and Privacy, the MDH Data Officer, the MDH Chief Information and Security Officer, and a representative from OCMP. Membership also includes the MDH Chief Technology Officer, the MDH Chief Information Officer, and the MDH Chief Compliance Officer in an advisory capacity.

a. Officers

The SDI Team is led by the Director of the Office of Internal Controls, Audit Compliance & Information Security (IAC/S). The Chair within their discretion may call an emergency meeting of the SDI Team for review of an agreement designated as an emergency.

b. Team Support

Health Policy Analysts assigned to the SDI Team are responsible for reviewing Data-Related Agreements for compliance with the policies and guidelines as set forth in MDH Policy 01.06.01.They shall also be responsible for updating and managing the weekly agendas, the SDI Shared Drive, and the Cognito Forms platform.

III. VOTING RIGHTS

Agreements are decided by a consensus vote amongst the four primary voters: the representative from the IAC/S Office of Compliance and Privacy, MDH Data Officer, MDH Chief Information and Security Officer, and the representative from OCMP. The MDH Chief Technology Officer, the MDH Chief Information Officer, MDH Chief Compliance Officer, and a representative from the Office of the Attorney General may participate as advisory members. In the absence of a primary voter, a designee assigned by the primary voter may take their place in the voting. If a Data-Related Agreement is submitted by a unit of a voting member, that voting member must abstain from voting on that Agreement. For example, if an Agreement is submitted for review by the Office of Internal Controls, Audit Compliance & Information Security the representative from the IAC/S Office of Compliance and Privacy will abstain from voting on that Agreement.

a. Lack of Consensus

In the event that the SDI Team is unable to reach a consensus determination regarding a Data-Related Agreement, the SDI Team shall provide the Secretary with a memorandum providing an explanation of the concerns with the Agreement. The Secretary will then determine if the agreement should be approved, denied, or granted a waiver per the requirements of MDH Policy 01.06.01.

IV. REVIEW OF SUBMISSIONS

The SDI Team shall review all Data-Related Agreements submitted to the SDI Team via Cognito Forms. Upon receiving documentation from a MDH unit, the SDI Team will complete their review of the proposed contract and provide results of the review to the submitting MDH unit. During the SDI Team review process, the submitter, or their designee, must be available to answer any questions either by phone or email to assist the SDI Team with their review.

a. Definitions

Terms have the same meaning as defined in MDH Data Use Policy (01.06.01).

b. Meetings

The SDI Team shall conduct, at a minimum, weekly meetings to review, discuss and vote on Data-Related Agreements. When a member of the SDI Team is unable to attend a meeting, they shall appoint a designee to serve in their absence and to vote on any agreements presented for a vote at the meeting.

c. Review Process

The SDI Team will aim to respond to submissions of Data-Related Agreements within 30 days from submission and receipt of all required documentation from the MDH unit or proposed Data Partner. Further, for complete review, the proposed Data Partner will be asked to a complete an IT Security Controls Survey to assess if the data partner has Appropriate Safeguards and Access Controls. In reviewing any Data-Related Agreements, the SDI Team will conduct a risk assessment as the agreement pertains to MDH Data. The risk assessment will consider the following elements:

1. Analysis of the requested Data to determine that MDH Data is not inadvertently shared beyond what is requested;

2. Review and classification of the Data that will be shared and the classification of such Data to determine privacy and BAA requirements;

3. Whether access to MDH Data has Appropriate Safeguards and Access Controls;

4. If MDH Data is being transferred to, stored in, or collected by systems or entities that are outside the control or responsibility of MDH;

5. Whether the transfer of Data to external parties or systems is required by law or the terms of a grant agreement (e.g., requirement for funding or mandated reporting); and

6. Whether any other controls or requirements are necessary to protect MDH Data.

d. Emergency Situations

Any emergency submissions will be reviewed by the SDI Team or SDI Chair on a case-by-case basis. Any member of the SDI Team may designate a Data-Related Agreement as an emergency by notifying the SDI Team by email. Upon designation as an emergency, one

member of the SDI Team may grant emergency approval of a Data-Related Agreement. Following emergency approval, the Data-Related Agreement shall be reported to the full SDI Team at the next standing meeting of the SDI Team or an emergency meeting if called by the Chair.

e. Outcomes

Review by the SDI Team can result in the following outcomes: approval, provisional approval, recommendation for a waiver from the Secretary, remand for additional information or correction, or denial.

i. Approval

Approval will only be granted if the SDI Team determines there are Appropriate Safeguards and Access Controls in place.

ii. Provisional Approval

In instances where Data cannot be stored or processed on systems that meet Appropriate Safeguards and Access Controls in accordance with State and MDH policies, provisional approval may be granted if the SDI Team determines that a Data-Related Agreement presents a low or medium risk to MDH Data and information security based upon internal review of current data and security safeguards and access controls. Provisional approval shall include a determination memo with risk remediation recommendations from the SDI Team that must be completed within one year. Failure to complete these recommendations within one year may result in the revocation of provisional approval as well as the denial of future renewal(s) of the Data-Related Agreement.

iii. Recommendation for Waiver from the Secretary

In instances where Data cannot be stored or processed on an Approved System, the SDI Team may request a waiver from the Secretary to permit such use, storage, or collection of MDH Data on a non-State Approved System. In determining if a waiver is appropriate, the SDI Team will consider any risks to MDH Data. The SDI Team shall provide the Secretary with a Memorandum providing recommendations as to why a waiver may be appropriate.

The Secretary shall review all recommendations by the SDI Team for a waiver; however, there is a presumption against the authorization of waivers. The Secretary shall determine in their discretion as to whether a waiver is appropriate based on all materials sent for review and the recommendations of the SDI Team. The Secretary shall provide written notification to the requesting MDH unit upon the authorization of a waiver.

iv. Remand for Additional Information or Correction

A remand for additional information or correction shall occur when the MDH unit does not submit appropriate or sufficient documentation for the SDI Team to complete their review.The SDI Team will need all proposed contracts and documentation to

appropriately review the proposed Data-Related Agreement. Once an MDH unit receives notice of a remand from the SDI Team, the submitting unit shall have 30 days to resubmit and correct information provided to the SDI Team. If 30 days have passed since the remand and the MDH unit has not provided the additional information or correction, the request shall be treated as a denial and will require a resubmission to the SDI Team for review.

v. Denial

If the SDI Team determines that there are not Appropriate Safeguards and Access Controls and waiver is not appropriate, the SDI Team may issue a denial. If a denial is issued, the SDI Team shall provide a memorandum to the submitting MDH unit that explains the reason for the SDI Team's denial. If adequate changes are made to cure the concerns of the SDI Team, the MDH unit may resubmit the Data-Related Agreement in Cognito Forms as a new submission.

f. Designation as a Trusted Data Partner

The SDI Team at their discretion can assess a data partner to determine if the data partner meets the criteria of a Trusted Data Partner. The SDI Team will initiate the Trusted Data Partner certification process on a case-by-case basis. If the SDI Team determines that the entity meets the requirement of a Trusted Data Partner, the SDI Team will send the recommendation to the Secretary for final approval. Upon designation, the Trusted Data Partner will receive a memorandum from the SDI Team indicating this status.

i. Minimum Security Standards

The SDI Team will review the proposed Trusted Data Partner for minimum security standards in including but not limited to:

- NIST SP 800-53 Rev.4 Standards
- MARS-E 2.2
- HIPAA Security Rule NIST SP 800-66 Rev.1
- State of Maryland IT Security Manual
- Industry Recognized Security Certification (e.g., HITRUST Certification)
- SOC 2 Type II Audit Report within the Last 12 Months.

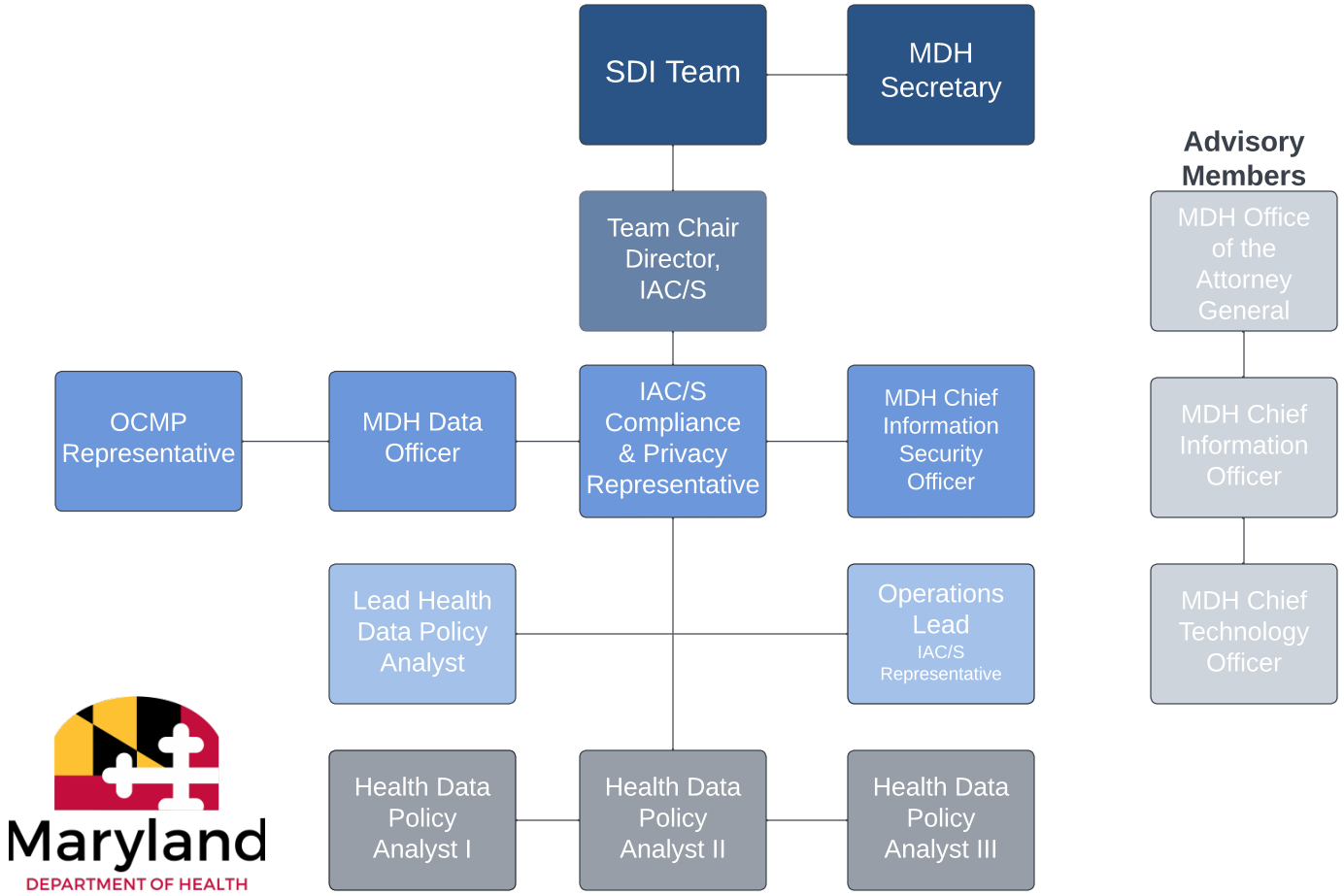
A Data Partner may be requested to provide a letter of attestation of these minimum security standards.

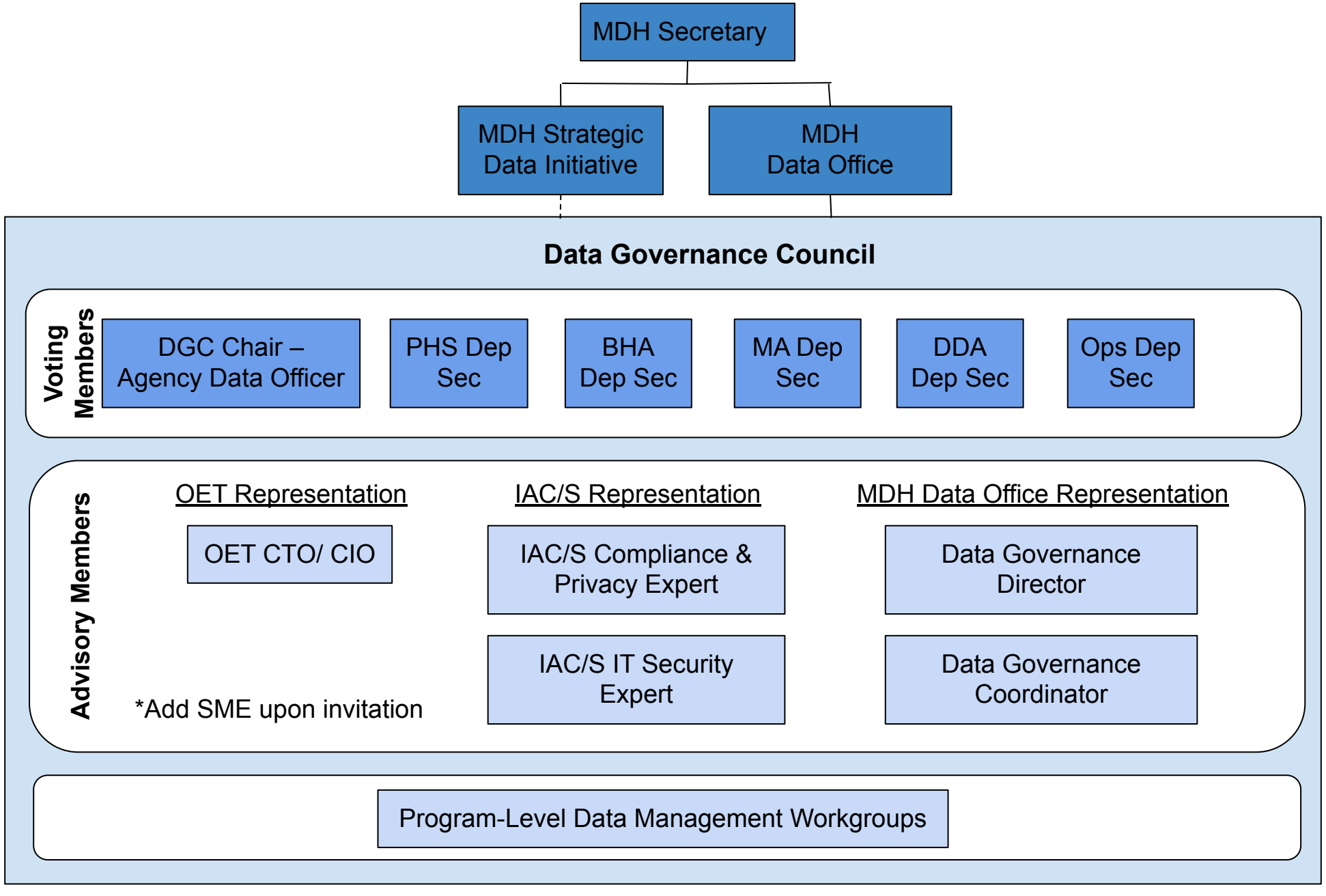
ii. Minimum Data Governance and Management Standards

The SDI Team will review the proposed Trusted Data Partner for minimum data governance and management standards including a master agreement with MDH that addresses data governance and management.

iii. Renewal Procedures
The status of a Trusted Data Partner shall be renewed annually or anytime there is a material change in the Trusted Data Partner's data environment to ensure the Trusted Data Partner remains in compliance with the requirements of this status as outlined in MDH Policy 01.06.03.

ATTACHMENT 3: SDI TEAM ORGANIZATIONAL CHART




MDH Secretary
MDH Strategic Data Initiative
MDH Data Office
Data Governance Council
Voting Members
DGC Chair – Agency Data Officer
PHS Dep Sec
BHA Dep Sec
MA Dep Sec
DDA Dep Sec
Ops Dep Sec
Advisory Members
OET Representation
OET CTO/ CIO
IAC/S Representation
IAC/S Compliance & Privacy Expert
IAC/S IT Security Expert
MDH Data Office Representation
Data Governance Director
Data Governance Coordinator
*Add SME upon invitation
Program-Level Data Management Workgroups