MDH POLICY

https://health.maryland.gov/Pages/mdhpolices.aspx

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

MDH POLICY 01.06.01
Version Effective: 12/15/2021

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 protection 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 use of MDH Data by Data Partners and Trusted Operational 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 also 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.

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

7. **"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.

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

9. **"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.

10. **"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.

11. "Protected Health Information" 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.

12. "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, MDH Privacy Officer, and a representative from the Office of Contract Management & Procurement (OCMP),or their designee(s). The MDH Chief Technology Officer and the MDH Chief Compliance Officer serve on the Team in an advisory capacity.

13. "Secretary" means the Secretary of the Maryland Department of Health.

14. "Trusted Operational Partner" means an entity essential to MDH operations and approved as a trusted partner by the SDI Team.

B. General Policy.

Data Partners and Trusted Operational 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 the effective date of this policy are subject to SDI review upon renewal of the agreement. Data-Related Agreements which cannot meet the standards as outlined in this policy requiring Data Use through a State Approved System 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 the effective date of this policy. 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 Operational Partners, MDH Units must still submit the agreement to the SDI Team via Cognito Forms. For Data-Related Agreements with Trusted Operational Partners or those required by statute, regulation, law, or grants, SDI will serve in an advisory capacity and provide non-binding recommendations regarding the proposed Data-Related Agreement to the submitting MDH Unit.

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, 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.

C. Additional Data Use Considerations

The hosting of MDH Data on State Approved Systems is one of many considerations for Data-Related Agreements. Additional considerations with such Data-Related Agreements 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 outlined 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).

IV. COMPLIANCE & 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 and Audit Compliance (IAC), or the Office of Human Resources as appropriate for Data-Related Agreements

that do not follow this policy.

In the event of 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.

B. MDH Chief Compliance Officer.

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

C. 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.

D. 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.

E. 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.

F. 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.

G. MDH Privacy Officer.

Assures 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 MDH Privacy Officer also reviews Data-Related Agreements to ensure MDH is protected in the event of a breach. The MDH Privacy Officer serves as a voting member of the SDI Team.

H. MDH Secretary.

The MDH Secretary designates the Chair of the SDI Team. Further, the Secretary must approve the individual designed 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.

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

MDH's Office of Contract Management and Procurement reviews and approves allagreements 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.

J. Strategic Data Initiative Team.

The Strategic Data Initiative (SDI) Team is led by a Chair who is selected by the Secretary. Voting members include the MDH Privacy Officer, 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 Team 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 Operational Partners.

K. MDH 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 Team.

VI. REFERENCES

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

- Maryland Department of Information Technology, State of Maryland Information Technology Security 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-%20IAP%20-%206-1-01.pdf

- 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 on Research Involving Human Subjects Involving the MDH Institutional Review Board (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

APPROVED:

Dennis R. Schrader, Secretary

December 15, 2021
Effective Date

Maryland
DEPARTMENT OF HEALTH

Strategic Data Initiative Agreement Review

Please complete this form to request the Strategic Data Initiative (SDI) Team's review of your data-related agreement with a potential data partner.

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.

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

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

What type of agreement is proposed? *

- ◯ Business Associate Agreement
- ◯ Memorandum of Understanding
- ◯ Interagency Agreement
- ◯ Data Use Agreement
- ◯ Other

What services are being performed under the agreement? *

Under the agreement, where will MDH data be accessed, used or stored? *

Are you seeking a waiver for this agreement?

◯ Yes ◉ No

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

Upload or drag files here.

Name *

Name of person completing form.

Title *

Title of person completing form.

Email *

Email of person completing form.

Submit

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 the MDH Privacy Officer, the MDH Data Officer, the MDH Chief Information and Security Officer, and a representative from OCMP. Membership also includes the MDH Chief Technology Officer and the MDH Chief Compliance Officer in an advisory capacity.

a. Officers

The SDI Team is led by a Chair as designated by the Secretary. 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: MDH Privacy Officer, MDH Data Officer, MDH Chief Information and Security Officer, and the representative from OCMP. The MDH Chief Technology Officer and MDH Chief Compliance Officer 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 and Audit Compliance the MDH Privacy Officer 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 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. 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 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 Team or an emergency meeting if called by the Chair.

e. Outcomes

Review by the SDI Team can result in the following outcomes: Approval, recommendation for 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. 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.

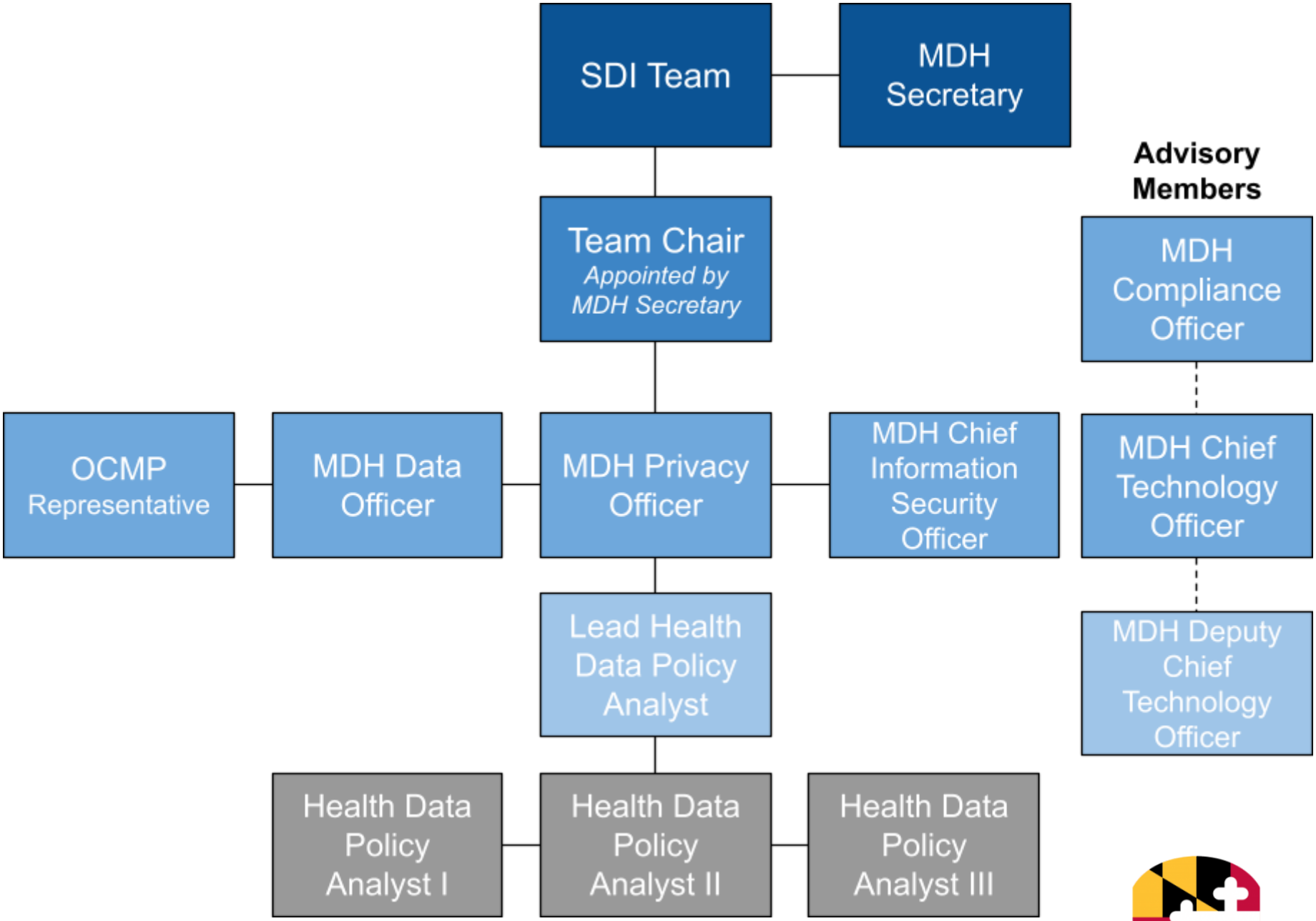
iii. Remand for Additional Information or Correction

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.

iv. 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.

ATTACHMENT 3: SDI TEAM ORGANIZATIONAL CHART



Maryland
DEPARTMENT OF HEALTH