Procedure Document: MPH Data Review Team and OCDO Privacy Board

Version: 2.0 (4/2023)

Contents

Procedure Document: MPH Data Review Team and OCDO Privacy Board

Version: 2.0 (4/2023)

1. Purpose

The purpose of this Procedure is to ensure that all Data exchanged and utilized by the Indiana Management Performance Hub meets appropriate business, legal, privacy, security, and technical needs prior to Data movement out of the MPH Protected Zone.

2. Applicability

This Procedure is internal to the Office of the Chief Data Officer (OCDO) and shall apply to all MPH activities related to the movement of Data out of the MPH Protected Zone.

This Procedure is put forth in the context and in furtherance of the *Office of the State Chief Data Officer: MPH Information Access Policy*.

3. Revision History

Version	Date	Name	Revision Description	Supersedes
1.0	7/2020	T. Cotterill	Initial version.	n/a
2.0	4/2023	T. Cotterill	Incorporates HIPAA Privacy Board obligations.	1.0

4. Ownership

Please direct questions and concerns to the following owner(s) of this Procedure:

1. MPH Legal, Privacy, & Security

5. Definitions

All defined terms used but not defined in this Procedure may be referenced in the Policy.

1. "Data" means electronically-recorded information, including Government Information.
2. "Government Information" has the meaning set forth in IC 4-3-26-7.
3. "Member" means relevant individuals associated with the positions identified in Paragraph 8.2 or as allowed by Paragraph 8.6 of this Procedure.
4. "MPH PZ" means the MPH Protected Zone.
5. "PMO" means staff within the MPH Project Management Office.
6. "Policy" means the *Office of the State Chief Data Officer: MPH Information Access Policy*
7. "Procedure" means this *Procedure Document: MPH Data Review Team and OCDO Privacy Board.*
8. "Protected Health Information" has the meaning set forth in 45 CFR 160.103.
9. "Violation" means all activities contemplated by the Procedure that are not expressly allowed by the Procedure.

6. Exceptions

All exceptions are considered procedural deviations and must be timely documented in Microsoft DevOps. Notwithstanding the requirements of Health Insurance Portability and Accountability Act of 1996 (HIPAA), exceptions may be granted by the MPH Data Review Team, subject to its policies and procedures, by the Chief Data Officer, or by the Chief Privacy Officer.

Exceptions may not be granted in the review of protected health information, where the MPH Data Review Team constitutes a Privacy Board under 45 CFR 164.512(i)(1)(i)(B). MPH Legal, Privacy, & Security will make such a determination.

7. Violations

Violation of this Procedure may constitute employee misconduct and will be addressed in accordance with applicable law and policy, including but not limited to the State Employee Handbook and the MPH Employee Handbook.

8. Procedure: MPH Data Review Team and OCDO Privacy Board

8.1. Background

The MPH facilitates the exchange and utilization of Data for research and community benefit initiatives. A core component of this responsibility is a thorough review of all Data exchange and utilization facilitated by the MPH. This review is conducted by the MPH Data Review Team and OCDO Privacy Board, which is dedicated to ensuring that Data is exchanged and utilized only in appropriate circumstances and with necessary controls in place.

8.2 Data Review Team and Privacy Board Membership

The MPH Data Review Team and OCDO Privacy Board consist of the following individuals:

- A representative of MPH Legal;
- the MPH Director of Information Security;
- the MPH Principal Data Scientist or Data Engineering Manager;
- the MPH Director(s) of Engagement and Analytics most closely associated with the proposed release (this may include multiple DEAs, all of which must approve); and
- the MPH Director of Enterprise Solutions.

8.3 Data Product Preparation for Review

Prior to a dataset being presented to the Data Review Team, all documentation relating to the request must be made available for review in the associated card. If applicable, this documentation will include:

- a link to the location within the MPH PZ of the Data to be reviewed;
- the name of Data file(s) to be reviewed;
- a list naming all State agencies and external partners with Data involved in the request;
- the requestor's DSA;

- a reference to the executed DSA(s) with the involved agency or agencies;
- the executed charter(s) with the involved agency or agencies;
- a data dictionary addressing all Data involved in the request (This includes Data contributed from an external partner in relation to the request.);
- the proposed means of Data provision (e.g., MPH Enhanced Research Environment); and
- the rationale for that means of Data provision (i.e., why is this the most secure and efficient Data transfer mechanism?).

8.4 Review Procedure Generally

Each Member of the MPH Data Review Team and OCDO Privacy Board review Data proposed for release from their unique perspectives. As a general matter, primary and secondary focuses of each reviewer are defined below:

- MPH Legal
    - Does this Data product comply with applicable legal and privacy requirements, from a legal and regulatory perspective?
    - Does this Data product meet the use case defined in the request, from a business and data quality perspective?
- MPH Security
    - Does this Data product comply with applicable security requirements under the "CIA" Triad?
    - Does this Data product meet the use case defined in the request, from a business and data quality perspective?
- MPH Data Science
    - Does this Data product align with applicable privacy requirements, from a quantitative perspective?
    - Does this Data product meet the use case defined in the request, from a data quality perspective?
- MPH Engagement
    - Does this Data product meet the use case defined in the request, from the business and data quality perspectives?
    - Does this Data product align with applicable privacy requirements, from a business perspective?
- the MPH Director of Enterprise Solutions
    - Does this Data product meet the use case defined in the request and align with organizational objectives?
    - Does this Data product align with applicable privacy requirements, from a business perspective?

The MPH Data Review Team and OCDO Privacy Board must consider degrees of identifiability of Data products, an inquiry that considers the granularity of the Data in question. The MPH offers the following classification scheme to guide this review.

1. Row-level identifiable
2. Row-level deidentified
3. Aggregate, no suppression applied
4. Aggregate and suppressed

The State of Indiana Information Privacy Policy offers general obfuscation guidance to agencies. This guidance is reproduced here, for use by the MPH Data Review Team and OCDO Privacy Board at its discretion.

> 1. In the case of aggregate information, suppress the information so that groups of "n" counts fewer than ten (10) are obfuscated and apply secondary suppression as needed to ensure that suppressed cells fewer than ten (10) may not be recalculated through subtraction using the remaining cells. Finally, consult the law or regulation which governs the information proposed for release and ensure that the data product either: 1) no longer constitutes a protected class of information; or 2) qualifies for a disclosure exception based on its content, the ultimate receiver, and the receiver's proposed use of the information.
> 2. In the case of row-level information, consult the law or regulation which governs the information proposed for release. Remove or obfuscate data elements in a manner so as to ensure that the data product either: 1) no longer constitutes a protected class of information; or 2) qualifies for a disclosure exception based on its content, the ultimate receiver, and the receiver's proposed use of the information.

State of Indiana Information Privacy Policy.

8.5 Approval Procedure

Approvals shall be timely documented in Microsoft DevOps by the Member offering that approval or, at the documented request of that Member, by the MPH PMO. Unanimous approval is required prior to the release of any Data from the MPH PZ. Once all approvals are documented and related documents fully executed, the Data may then be exchanged with the requestor or utilized outside of the MPH PZ through the means defined in the request. In no event may Data be exchanged with the requestor prior to full execution of the requestor's DSA.

8.6 Absence of Member

In the event of a planned absence of a Data Review Team Member, that Member should delegate his/her review to another MPH employee with similar duties and expertise. Such delegations must be documented in the card with the related approval.

In the event of an unplanned absence of a Data Review Team Member, remaining Members of the Data Review Team will meet to unanimously agree on a suitable proxy for that Member. Such delegations must be documented in the card with the related approval.

8.7 Export from Enhanced Research and Analytics Environments

Following approval under this Procedure, Data exchanged with requestors will, by default, be made available within an environment approved by the MPH for this purpose. A request to export Data from the environment is subject to secondary review by the MPH. As a general matter, requests for export should involve Data products that are no more granular than Tier 4, Aggregate and suppressed, as identified in Sec. 8.4 of this Procedure. Approvals required for export requests are limited to MPH Legal, MPH Data Science, and MPH Engagement.

9. HIPAA Privacy Board: Additional Obligations

9.1 HIPAA Privacy Board Member Obligations

In facilitating the exchange of Protected Health Information, Members constitute a privacy board that:

1. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
2. Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
3. Does not have any member participating in a review of any project in which the member has a conflict of interest.

45 CFR 164.512(i)(1)(i)(B).

If the MPH is conducting the research internally, the OCDO shall consult with appropriate HIPAA covered entities to determine whether adequate separation exists to comply with the requirements of 45 CFR 164.512(i)(1)(i)(B)(2).

9.2 Review Procedure: Additional Requirements for OCDO Privacy Board

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes specific obligations on a privacy board. These obligations are restated here in part and shall serve as a checklist for the OCDO Privacy Board in its review of Protected Health Information. In this capacity, the OCDO Privacy Board reviews the Data requested in the context of the research protocol and, if appropriate, approves an

alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of Protected Health Information.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the… privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the… privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(1) An adequate plan to protect the identifiers from improper use and disclosure;

(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the… privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

...

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the… privacy board, as applicable.

45 CFR 164.512(i)(1)(ii)-(i)(2).

10. References

1. Cotterill, *State of Indiana Information Privacy Policy*.
2. Russell Densmore, *Privacy Program Management: Tools for Managing Privacy Within Your Organization* at 167 (2d ed. 2019).