This DATA SHARING AGREEMENT is effective as of the date of approval by the chief privacy officer, as evidenced in Sec. 6, between the [Agency 1 Name] [(Agency 1 Acronym)] and the [Agency 2 Name] [(Agency 2 Acronym)].

# CONTACT INFORMATION

[Agency 1 Name]

[Name]

[Title]

[Address]

[Email]

[Name of Agency 1 Agency Privacy Officer]

[Email of Agency 1 Agency Privacy Officer]

[Agency 2 Name]

[Name]

[Title]

[Address]

[Email]

[Name of Agency 2 Agency Privacy Officer]

[Email of Agency 2 Agency Privacy Officer]

# DATA EXCHANGE

## Definitions.

## “APO” means the relevant agency privacy officer designated in each business unit under *State of Indiana Policy: Information Privacy* and identified in Sec. 1 of this DSA.

## "Data " means the collection of electronically-recorded information, inclusive of all individual data elements, exchanged between the parties by virtue of this DSA.

## "DSA" means this data sharing agreement.

## "OCDO" means the Office of Chief Data Officer established by Ind. Code § 4-3-26-9.

## Authorization. Data exchange as contemplated in this DSA occurs in accordance with Ind. Code Ch. 4-1-6-2(13), which provides, in part, as follows: A state agency shall exchange with other agencies official personal information that it has collected in the pursuit of statutory functions when (check one):

[ ] the information is requested for purposes authorized by law including a rule promulgated pursuant to IC 4-22-2;

[ ] the data subject would reasonably be expected to benefit from the action for which information is requested (requires individualized benefit to the data subject);

[ ] the exchange would eliminate an unnecessary and expensive duplication in data collection and would not tangibly, adversely affect the data subject; or

[ ] the exchange of information would facilitate the submission of documentation required for various state agencies and departments to receive federal funding reimbursement for programs which are being administered by the agencies and departments.

## Written Justification of Authorization. [Include a written statement supporting use of the authorization selected in Sec. 2.b. above. Provide citations, where appropriate.]

## Purpose and Objectives. [Include a written statement articulating the purpose and objectives of the Data exchange contemplated in this DSA.]

## Additional Agreement Terms. [Use this field only if needed to memorialize additional terms and conditions required by State or Federal law or regulations. Provide citations for this requirement.]

## Term and Termination. This DSA is effective as of the date of approval by the chief privacy officer, as evidenced in Sec. 6, and shall continue until: 1) terminated pursuant to Sec. 2.f.a.; 2) the date identified in Sec. 2.f.b.; or 3) on December 31 of the calendar year following execution, whichever occurs first.

## This DSA may be terminated by the parties or the OCDO at any time and for any purpose. Termination is effected by providing written notice to the other-party contact listed in Sec. 1 *and* to the OCDO by email to ResponsibleData@mph.IN.gov. The terminating party shall strive to provide reasonable advance notice under this subsection. If termination were to occur, the OCDO will consult with the parties regarding related data needs.

## Date of Termination: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## On termination of this DSA, the receiving party shall, within thirty (30) days of termination, securely dispose of the Data and its derivatives. In so doing, the receiving party shall, unless legally prohibited, destroy all of the Data and its derivatives in its systems or otherwise in its possession or under its control, in all of its forms. The Data shall not be recoverable, using the “clear” method of sanitization defined in NIST Special Publication 800-88 Rev.1. The receiving party further agrees that it will overwrite the logical storage location of the Data as well as all user-addressable locations of the Data.

## The receiving party agrees to memorialize such destruction through completion and submission to the other party *and* the OCDO of the certificate of destruction prescribed by the OCDO at <https://www.in.gov/mph/cdo/files/State-of-Indiana-Internal-COD.docx>.

# PRIVACY, DATA PROTECTION, AND INCIDENT RESPONSE

## Governing Citations.

## Ind. Code Ch. 4-1-6, governing information sharing and confidentiality.

## Ind. Code Ch. 4-1-10, governing the release of social security numbers (as applicable).

## Ind. Code Ch. 4-1-11, governing security breach involving a state agency.

## Ind. Code § 5-14-3-6.5, governing confidentiality.

## Additional Governing Citations.

## [Agency enabling statutes]

## [Agency-specific statutes governing Data (if any)]

## Data Use. Data shall be leveraged to further the purposes of this DSA, but only in accordance with its terms. Nonconforming uses may subject the violating party to termination of the Data exchange enabled by this DSA, pursuant to Sec. 2.f. and may further initiate a privacy impact assessment of the relevant system or systems.

## Storage Location. The parties have considered the benefits and risks of duplication of Data for the purposes of this DSA. [Select one of the following options.]

## [ ] Data subject to this DSA will be maintained on information technology infrastructure owned or licensed by the Office of Technology, excluding agency analytics environment infrastructure described immediately below.

## [ ] Data subject to this DSA will be maintained in an agency analytics environment, as defined in and pursuant to *State of Indiana Policy: Fair Information Practices related to Agency Analytics Environments*.

## [ ] Data subject to this DSA will be maintained on information technology infrastructure owned or licensed by the receiving agency.

## [ ] Other.

## [Include a written statement to describe and support the selection made above.]

## Data Protection.

## Data subject to this DSA will be maintained in accordance with applicable law.

## Data subject to this DSA will be protected by appropriate administrative, physical, and technical security measures to safeguard against unauthorized access, disclosure, or theft.

## Data subject to this DSA will be transmitted through a managed file transfer platform approved by the Indiana Office of Technology for that purpose, using secured encryption technologies that meet or exceed the standards under Federal Information Processing Standards (FIPS) 140-2, Level 1, for data in motion.

## Data subject to this DSA will be maintained at rest using an environment approved by the Indiana Office of Technology for that purpose, in accordance with secured encryption technologies that meet or exceed the standards under FIPS 140-2 and National Institute of Standards and Technology (NIST) 800-131A Rev. 1.

## Data subject to this DSA will be maintained at rest solely in data centers in the continental United States of America, shall not be maintained on portable devices, including personal laptop and desktop computers.

## Data subject to this DSA:

## [ ] may

## [ ] may not

## be accessed by a third-party under contract with the receiving party.

## \* (Note that this does not govern individual temporary staffing resources designated through the Selected Resource Program under the Indiana Managed Service Provider program, Contract No. 58993, which are akin to state employees for the purposes of information governance.)

## Notification of Breach of Security. If there is a breach of the security of the system (as defined in Ind. Code Ch. 4-1-11-2) involving Data, the party having control of the Data subject to the breach shall promptly:

## institute all appropriate and necessary mitigating actions required by applicable State and Federal laws and regulations;

## comply with all disclosure and notification actions required by applicable State and Federal laws and regulations;

## notify the Indiana Office of Technology via email to the Indiana Security Incident Response Team at isirt@iot.IN.gov;

## notify the other-party contact listed in Sec. 1 of this DSA;

## make reasonable efforts to cooperate with the requests of the other-party contact listed in Sec. 1 of this DSA; and

## following any necessary mitigation, disclosure, and notification activities, the APO must provide to the State CPO documentation of actions taken, pursuant to *State of Indiana Policy: Information Privacy*.

# Partnership Management

## Amendments. No alteration or variation of the terms of this DSA are valid unless made in writing, signed by the parties hereto, and approved by the OCDO. No oral understanding or agreement not incorporated herein shall be binding on the parties.

## Funding. No funding mechanism or agreement is contemplated or reached by this DSA. If necessary, funding terms needed to carry out the purpose of this DSA will be agreed upon by the parties and will be memorialized in a memorandum of understanding between the parties pursuant to FMC 3.4.

# Change Control

Without exception, list below any sections of this DSA that have been modified or deleted from the State’s standard data sharing agreement, as published at <https://www.in.gov/mph/cdo/files/State-of-Indiana-Internal-DSA.docx>.

* [Create this list only if needed to reflect modifications, as noted above.]

# APPROVALS

IN WITNESS WHEREOF, the parties have executed this DSA by their duly authorized officers or representatives on the date set forth below, effective as of the date of approval by the chief privacy officer, as evidenced below.

[AGENCY 1 NAME]
[AGENCY 1 SIGNATORY NAME]
[AGENCY 1 SIGNATORY TITLE]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date: \_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_
APO INITIALS

[AGENCY 2 NAME]
[AGENCY 2 SIGNATORY NAME]
[AGENCY 2 SIGNATORY TITLE]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date: \_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_
APO INITIALS

**APPROVED:**

\_\_\_\_\_\_\_\_\_\_\_\_\_
Chief Privacy Officer

Date: \_\_\_\_\_\_\_\_