**DEPARTMENT OF CHILDREN AND FAMILIES**

Division of Management Services

**Application for DCF Data**

This application is the first step in the data request process at the Department of Children and Families. Your request will be vetted by the appropriate DCF data steward and other subject matter experts to determine whether or not the request is consistent with the DCF mission (<https://dcf.wisconsin.gov/dcf-mission-goals-values>) and has the potential to inform improvements in DCF.

Personal information you provide may be used for secondary purposes [Privacy Law, s. 15.04(1)(m), Wisconsin Statutes].

**Contact Information**

|  |  |
| --- | --- |
| Name of Requestor(s)      | Position/Title            |
| Telephone Number (Home)      | Cell Phone      | Fax Number |
| Address – (Street, City, State, Zip Code) | Email address |
| **Agency/Education/Business Affiliation**      |       |        |
| Name of Organization      | Telephone Number (Office)       | Fax Number |
| Address—(Street, City, State, Zip Code) | Email Address |  |

**General Data Request Information**

1. Is this data request (check all that apply):

 [ ]  To fulfill work requested by DCF

 [ ]  Part of degree/course work (if yes, please specify)

 [ ]  Ph.D. [ ]  Master’s Degree [ ]  Bachelor’s Degree [ ]  Other

 [ ]  Grant funded

 [ ]  For publication

 [ ]  Program evaluation

 [ ]  Government sponsored / monitored

 [ ]  ECIDS Data Request

 [ ]  IRP’s MSPF Request

1. Which of the following best describes the type of data that you are requesting?

[ ]  Aggregate Data: counts of persons or families by categories (e.g. number of program participants by county, age group, and month).

[ ]  Individual Data: specific data on persons or families (e.g. county, age group, and month of each program participant)

1. Are you requesting any data from other Wisconsin state agencies? [ ]  Yes [ ]  No

If yes, please explain.

**Project Information**

1. Summarize the principal purpose of your project.

1. Describe your project by providing a detailed plan. Please include specific research questions or hypotheses to be tested and the study design (if applicable). Also include a description of study groups (cases, controls, as appropriate), data collection methods and analytic plan (attach additional sheets when necessary).

1. Explain how your project contributes to the mission of DCF (<https://dcf.wisconsin.gov/dcf-mission-goals-values>) to promote the economic and social well-being of Wisconsin’s children and families.

1. List all variables or categories of data that you are requesting. For each variable, provide a brief explanation as to how it will be used to address your specific research questions or hypotheses. Please attach an Excel template that details the data elements you are requesting and the format you would like them in.

1. Indicate the months/years for which you are requesting data.

1. Is Personally Identifiable Information (PII) required: [ ]  Yes [ ]  No

(Definition of PII: Personally Identifiable Information (PII) is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.)

6a. If you answered “Yes” to question 6, please identify the data elements that are PII and explain why they are required for your research.

1. Describe the security and storage protection mechanisms to be used in your project (see the DCF standard legal language for storage protection mechanisms in Appendix A). How will individual record data obtained through this application be stored and maintained? Specifically describe the mechanisms for insuring that data will not be re-released or copied and for limiting access to individuals named in this application.

**NOTE: that submission does not guarantee approval of requests. All requests will be routed through the DCF External Request Recommendation Process.**

|  |
| --- |
| **Office Use Only:****External Request ID #:**       **Date Received:**       |

**Appendix A: DCF Standard Data Protection Mechanisms**

REQUIREMENTS TO RECEIVE INFORMATION

All requests by the recipient agency for information or access to information systems and data bases shall be coordinated through the DCF Data Steward(s) (See Appendix A) for the source agency. These personnel shall respond in a timely manner to requests for information or access to information systems and data bases.

If specific requests by the recipient agency for information are denied or only partially granted by the source agency, the source agency shall provide an explanation of the reasons for the denial or limitation.

The recipient agency agrees to make all staff with access to data and information under this agreement aware of the contents of this agreement, state and federal confidentiality requirements, and the consequences of violating those confidentiality requirements.

The recipient agency agrees to store information received under this agreement in a secure manner in accordance with NIST special publications 800-53 (Rev. 4) - Minimum Security Controls (Moderate-Impact Baseline), limiting access to information only to the staff identified in Appendix B. For online access to information, the recipient agency agrees to implement internal controls to prevent unauthorized access to the information system or data as authorized by this agreement.

The recipient agency agrees to permit authorized personnel of the source agency to make on-site inspections to ensure adherence to requirements of this agreement.

CONFIDENTIALITY: SECURITY DUTIES AND OBLIGATIONS AND LEGAL DISCLOSURE REQUIREMENTS

The recipient agency agrees to comply with all applicable state and federal laws, regulations, administrative memos and handbooks pertaining to the confidentiality of [program area(s)] information. The recipient agency is responsible for complying with all changes in confidentiality requirements that take place after the Agreement is in place.

The recipient agency agrees to comply with the following measures to protect the confidentiality of any information provided under this Agreement and to protect such information against unauthorized access or disclosure, and specifically agrees that [it will]:

A. Information subject to this Agreement shall be used only to the extent necessary to assist in the purposes in Article III and shall be disclosed only for the purposes defined in this Agreement;

B. Store all data, including access passwords or login information, in a place electronically and physically secure from access by unauthorized persons. Data storage shall be in compliance with the National Institute of Standards and Technology (NIST) special publications 800-53 (Rev. 4) - Minimum Security Controls (Moderate-Impact Baseline), under its current revisions;

C. Only store any digital copies of the Information received from DCF on [Recipient Agency Name] managed systems (including backup images or replicas), and shall not at any time utilize 3rd party, outside vendor, or cloud-based service providers for storage or transfer of Information received from DCF;

D. Use the data only for purposes authorized by law and this Agreement;

E. Not disclose data without prior written authorization from DCF;

F. Store and process the data in an electronic formation in a way that is secure from access by unauthorized persons;

G. Take precautions to ensure that only authorized personnel have access to the computer systems in which the data is stored;

H. Make the data accessible only to those staff of the recipient agency who require the data in the official performance of the job duties and for the specific purposes stated in this Agreement;

I. Instruct all persons with access to the data on the confidentiality requirement of the Agreement, and the sanctions for unauthorized disclosure of information;

J. Maintain a system sufficient to allow a complete and efficient audit of compliance within these safeguard provisions and the other requirements of this Agreement, including complete records of all use and disclosure and limitations on such use and disclosure, and allow random audits by the source agency;

K. Apply requirements regarding confidentiality of information as set forth in applicable state statutes, administrative rules, employee handbooks, and policy manuals equally to information obtained pursuant to this Agreement;

L. Prohibit the storage or transport of the data by means of unprotected media, such as (but not limited to) unencrypted laptop computers, tablets, iPads, mobile phone or Blackberry devices, unencrypted flash drives, unencrypted CD-ROMs, floppy disks, or the equivalent of these items;

M. Personnel with online access shall access information using only their personally assigned user IDs. Sharing of IDs is prohibited;

N. The recipient agency shall notify the source agency as soon as practicable, but shall not exceed 2 businesses days, if personnel with on-line access leave employment or change job functions so that user IDs can be promptly deleted.

The obligations of confidentiality assumed by the recipient agency pursuant to this Agreement shall not apply to the extent that the recipient agency can demonstrate that such information:

A. Is part of the public domain without any breach of this Agreement by the recipient agency;

B. Is or becomes known on a non-confidential basis, through no wrongful act of the recipient agency;

C. Was known by the recipient agency prior to disclosure hereunder without any obligation to keep it confidential;

D. Was disclosed to the recipient agency by a third party which, to the best of the recipient agency’s knowledge, is not required to maintain its confidentiality;

E. Was independently developed by the recipient agency; or

F. Was the subject of a written agreement whereby DCF consents to the disclosure of such confidential information by the recipient agency on a non-confidential basis.

If the recipient agency or any of its representatives shall be under a legal obligation, in any administrative, regulatory or judicial circumstance, to disclose any Confidential Information, the recipient agency shall give the State prompt notice thereof (unless it has a legal obligation to the contrary) so that the State may seek a protective order or other appropriate remedy. In the event that such protective order is not obtained, the recipient agency or its representative shall furnish only that portion of the information that is legally required and shall disclose the Confidential Information in a manner reasonably designed to preserve its confidential nature

DESTRUCTION OF RECORDS AND DATA

Unless authorized by DCF to retain data, the recipient agency shall destroy all records and data, regardless of format, no later than 60 days after the completion of the project or end of this agreement. Only reports that have been specifically approved for public release and that contain aggregate and summary information may be retained by the recipient agency.

All data destruction activities will be verified to the source agency by the recipient agency via a signed, dated and witnessed report. A witness for this action is defined as a second responsible person other than the Senior Information Security Officer (SISO), or similar, position.