DATA SHARING AGREEMENT

BETWEEN THE

WISCONSIN DEPARTMENT OF CHILDREN AND FAMILIES

AND THE

{RECIPIENT AGENCY}

Date

**I. PARTIES TO AGREEMENT**

The parties to this Agreement are the Department of Children and Families (DCF) (hereinafter referred to as the source agency) and the [recipient agency name] (hereinafter referred to as the recipient agency). DCF is the state agency responsible for the oversight and implementation of human service programs across Wisconsin including child welfare, child support, child care subsidies, child care regulation, child care quality and Temporary Assistance for Needy Families (TANF).

[Description of Program(s), Bureau(s) or Division(s) as appropriate]

[Recipient agency name and description of organization]

**II. DEFINITIONS AND PURPOSE OF EXCHANGE AGREEMENT**

1. **Definitions**

*“Confidential Information*” means all tangible and intangible information and materials accessed or disclosed in connection with this Agreement, in any form or medium (and without regard to whether the information is owned by the source agency or by a third party), that satisfy at least one of the following criteria:

* 1. Personally Identifiable Information (PII), as defined below;
	2. Non-public information related to the source agency’s staff, customers, technology (including data bases, data processing and communications networking systems), schematics, specifications, and all information or materials derived there from or based thereon;
	3. Information designated as confidential in writing by the source agency;
	4. Information prohibited from disclosure by federal law, including but not limited to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232 & 34 CFR Part 99, and 42 CFR Part 2; and the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Part 160 and part 164, Subparts A and E;
	5. Information prohibited from disclosure by Wisconsin statute, including but not limited to Wis. Stats. §§ 48.396 (court and law enforcement records), 48.78 (agency records about an individual who is or was in its care or legal custody), 48.981(7) (child protective services reports and records), 49.83 (public benefits information), 51.30 (treatment records), 118.125 (pupil records), 146.82 (patient health records), 938.396 (juvenile court and law enforcement records), and 938.78 (agency records about an individual who is or was in its care or legal custody).

*“Personally Identifiable Information (PII)”* means information that can be associated with a particular individual through one or more identifiers or other information or circumstances, including but not limited to the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable:

* 1. The individual’s last name on its own or in combination with the individual’s first name or first initial;
	2. The individual’s date of birth;
	3. The individual's Social Security number;
	4. The individual's driver's license number or state identification number;
	5. The number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account;
	6. The individual's DNA profile; or
	7. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.
1. **Purpose of Agreement**

The purpose of this Agreement is to address the policies, security and confidentiality issues**,** extraordinary costs, and processes to facilitate sharing [description of] data and information between the parties.

This Agreement allows designated staff of the recipient agency to be provided with [description of] data and information maintained by the source agency. Access to the data and information shall be arranged by the data stewards identified in Appendix A. The specific staff authorized to receive data and information and the type of access for the recipient agency is delineated in Appendix A. Access to data and information is permitted only for legitimate operations under this Agreement, as defined under Article III.

This Agreement requires compliance by the parties with all state and federal laws, administrative codes, and regulations, specifically, the National Institute of Standards and Technology (NIST) special publications, under their current revisions 800-53 (Rev. 5) - Minimum Security Controls (Moderate-Impact Baseline). Legal emphasis includes, but is not limited to, [INSTRUCTIONS TO DRAFTER: PLUG IN THE APPLICABLE DIVISION’S LANGUAGE HERE FROM BELOW][plug in applicable language from below based on division] and related administrative rules, memos, and handbooks, including but not limited to [Program related regulations]

[DSP/DMCPS: Chapters 19, 48, 49, 51, 55, 118, 146 and 938, Wis. Stats, Titles IV-B and IV-E of the Social Security Act, the Child Abuse Prevention and Treatment Act (CAPTA), the Family Educational Rights and Privacy Act (FERPA), 42 CFR Part 2 and HIPAA.]

[W-2: Chapter 49 Wis. Stats and Title 45 Public Welfare, Federal Code of Regulations.]

[DECE: Chapters 48 and 49, Wis. Stats, and Title 45, Code of Federal Regulations.]

[Child Support: Chapters 49 and 767 Wis. Stats, Title IV-D of the Social Security Act]

This Agreement shall remain in effect from [effective begin and end dates] unless the Agreement is suspended under the terms set forth in Article X.

**III. SCOPE OF AGREEMENT**

This Agreement allows the source agency to share information with the recipient agency for the purpose(s) of [describe data sharing purpose].

The Agreement allows the source agency to provide information on [describe what is being shared], to the extent permitted by the terms of this Agreement and applicable law. The source agency approves the use of [describe] data for the purpose(s) stated above.

The information provided by the source agency may contain PII. [The PII may be used for purposes of matching individual-specific data consistent with the purpose(s) stated above.] The recipient agency is not authorized to release PII or to contact individuals using the PII without the prior written approval of the source agency, and [other party, e.g., the county agency responsible for the case as appropriate].

The specific information that will be provided by the source agency is described in Appendix B to the Agreement.

**IV. 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 source agency’s Data Steward(s) (See Appendix A). These staff 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. 5) - Minimum Security Controls (Moderate-Impact Baseline), limiting access to information only to the staff identified in Appendix A. 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 staff of the source agency to make on-site inspections to ensure adherence to requirements of this Agreement.

The recipient agency must instruct all staff and staff of contractors or subcontractors with access to information covered under this Agreement regarding the safeguarding of confidential individuals’ information required by state and federal law. Training must precede any request for access and refresher training must be conducted once per year. The training must be documented by an acknowledgement and verification form.

Training may be accomplished by providing staff with confidentiality and security policy materials, such as those provided by the source agency, and requiring those materials to be read.

Training must be documented by requiring each staff of the recipient agency and any contractor or subcontractor to sign an acknowledgement and verification stating that they have received and read the materials, understand them, and agree to comply with them.

The acknowledgement and verification must be maintained by the recipient agency and be made available upon request for monitoring purposes.

**V. CONFIDENTIALITY: SECURITY DUTIES AND OBLIGATIONS AND LEGAL DISCLOSURE REQUIREMENTS**

Except as otherwise authorized by law, recipient agency may not disclose Confidential Information for any purpose other than purposes associated with this Agreement.

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:

1. Only use information subject to this Agreement to the extent necessary to assist in the purposes in Article III and shall be disclosed only for the purposes defined and allowed in this Agreement;
2. 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 NIST special publications 800-53 (Rev. 5) - Minimum Security Controls (Moderate-Impact Baseline), under its current revisions;
3. Only store any digital copies of the Information received from source agency on recipient agency 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 source agency;
4. Use the data only for purposes authorized by law and this Agreement;
5. Not disclose data without prior written authorization from source agency;
6. Store and process the data in an electronic formation in a way that is secure from access by unauthorized persons;
7. Take precautions to ensure that only authorized staff have access to the computer systems in which the data is stored;
8. 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;
9. Instruct all staff with access to the data on the confidentiality requirement of the Agreement, and the sanctions for unauthorized disclosure of information;
10. 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;
11. Apply requirements regarding confidentiality of information as set forth in applicable state statutes, administrative rules, staff or employee handbooks, and policy manuals equally to information obtained pursuant to this Agreement;
12. 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;
13. Ensure that staff with online access shall access information using only their personally assigned user IDs. Sharing of IDs is prohibited; and
14. Notify the source agency as soon as practicable, but after no more than two (2) businesses days if staff or former staff 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:

1. Is part of the public domain without any breach of this Agreement by the recipient agency;
2. Is or becomes known on a non-confidential basis, through no wrongful act of the recipient agency;
3. Was known by the recipient agency prior to disclosure hereunder without any obligation to keep it confidential;
4. 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;
5. Was independently developed by the recipient agency; or
6. Was the subject of a written agreement whereby source agency 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 source agency prompt notice thereof (unless it has a legal obligation to the contrary) so that the source agency 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.

**VI. Duties With Respect To Breach: UNAUTHORIZED USE, dISCLOSURE OR LOSS, Indemnification and equitable relief**

If the recipient agency becomes aware of any threatened or actual use or disclosure of any data or information that is not specifically authorized by this Agreement, or if any data or information is lost or cannot be accounted for, the recipient agency shall notify source agency as soon as practicable, but shall not exceed one (1) business day from the time that the recipient agency becomes aware of such use, disclosure, or loss. Such notice shall include, to the best of the recipient agency’s knowledge at that time, the persons affected, and the data or information disclosed.

The recipient agency will take the following steps with concurrence from source agency:

1. The recipient agency shall take immediate steps to mitigate any harmful effects of any unauthorized use, disclosure, or loss. The recipient agency shall reasonably cooperate with source agency’s efforts to seek appropriate injunctive relief or otherwise prevent or curtail any threatened or actual breach, or to recover its Confidential Information, including complying with a reasonable corrective action plan;
2. The recipient agency shall notify the affected individuals by mail or by a method previously used by source agency to communicate with the individual. If the recipient agency cannot with reasonable diligence determine the mailing address of the affected individual and source agency has not previously communicated with that individual, the recipient agency shall provide notice by a method reasonably calculated to provide actual notice;
3. The recipient agency shall notify consumer reporting agencies of the unauthorized release;
4. The recipient agency shall offer credit monitoring and identity theft insurance to affected individual(s) from a company, and under terms, acceptable to source agency for one (1) year from the date the individual(s) enroll(s) in credit monitoring;
5. The recipient agency shall provide a customer service telephone line or hotline to receive telephone calls and provide assistance and information to affected individual(s) during hours that meet the needs of the affected individual(s), as established by source agency; and
6. The recipient agency shall adequately staff customer service telephone lines to assure an actual wait time of less than five (5) minutes for callers.

Pursuant to this Agreement and Wis. Stat. §§ 893.82 and 895.46(1), in the event of a breach of the Agreement requirements on confidentiality by the recipient agency, the recipient agency shall indemnify and hold harmless the State of Wisconsin, source agency and its officers, staff or agents from any claims arising from the acts or omissions of the recipient agency, and its staff and agents, including but not limited to the costs of monitoring the credit of all persons whose Confidential Information was disclosed, disallowances or penalties from federal oversight agencies, any court costs, expenses, and reasonable attorney fees, and other costs incurred by source agency for its actual staff time and other costs associated with source agency’s response to the unauthorized use or disclosure constituting the breach.

The recipient agency shall indemnify and hold harmless the State of Wisconsin, source agency and its officers, staff or agents from any data released publicly or retained according to the Agreement, whether authorized or not.

The recipient agency acknowledges and agrees that the unauthorized use, disclosure, or loss of Confidential Information may cause immediate and irreparable injury to the individual(s) whose information is disclosed and to source agency, which injury will not be compensable by money damages and for which there is not an adequate remedy available at law. Accordingly, the parties specifically agree that source agency, on its own behalf or on behalf of the affected individual(s), shall be entitled to obtain injunctive or other equitable relief to prevent or curtail any such breach, threatened or actual, without posting security and without prejudice to such other rights as may be available under this Agreement or under applicable law.

**VII. SHARING INFORMATION WITH THIRD PARTIES**

The recipient agency is prohibited from sharing any data or information received from the source agency. If such a requirement or need is foreseen or arises, a written, signed and dated agreement must be in place with the third party vendor prior to any data transfer being made.

The provisions of this Agreement apply equally to any third party, vendor, contractor, or subcontractor that the recipient agency allows to use data and information available under this Agreement.

The recipient agency shall provide prior notice to the source agency of intended contractual relationships with third parties or vendors who may have access to data and information under this Agreement. The notification shall include the nature of the relationship, the types of information that will be shared and the planned use of the information by the third party or vendor.

The recipient agency is required to have agreements in place with the third party or vendor to ensure that the terms of this information sharing Agreement are enforced with the third party or vendor. The source agency reserves the right to approve the contents of such third party or vendor agreements.

The recipient agency is accountable for any violations of this information sharing Agreement committed by the vendor or third party. The recipient agency shall ensure that the third party or vendor instructs all staff/providers with access to the information regarding the terms of the information sharing Agreement and the confidential nature of [program area] information.

**VIII. PRODUCTS PRODUCED FROM DATA**

The recipient agency and its affiliates are authorized to produce reports, documents, and electronic files using information under this Agreement and as allowed by this Agreement for any project related to the purpose of this Agreement as described in Article III of this Agreement.

Reports, documents, and electronic files that contain aggregate and summary information, and do not contain PII, or information from which personal identity can be inferred, created with data provided under this Agreement and defined in Article III may be produced for internal use by the recipient agency.

Reports, documents, and electronic files that contain aggregate and summary information, and do not contain PII, or information from which personal identity can be inferred, may be produced for public distribution with the prior notification to the source agency. The source agency shall be notified at least ten (10) business days prior to the distribution and have the opportunity for advance review of any news releases, reports, documents, and files produced using information under this Agreement. The source agency shall receive a final copy of all reports or documents at least 24 hours prior to the release to the public.

Reports, documents, and electronic files that contain PII, or information from which personal identity can be inferred, created with data provided under this Agreement may be produced for internal use by the recipient agency with the prior approval of the source agency. Any internal use or distribution by the recipient agency shall be limited to persons necessary for the purposes for which the internal use or distribution is made. The specific use and distribution of the reports, documents, or electronic files shall be approved by the source agency prior to internal use by the recipient agency and its affiliates.

The source agency reserves the right to require changes in reports, documents or electronic files produced by the recipient agency if the reports or files inaccurately portray the [program area(s)] services provided by the source agency, if the reports or files portray an inappropriate level of detail that would compromise the confidentiality of individually identifiable information, or if the source agency has another reasonable basis for requiring a change.

All data files which are comprised of information under this Agreement shall be the property of the source agency and the recipient agency cannot claim proprietary rights to nor otherwise restrict public use of the data files, except to maintain the confidentiality of data provided under the terms of this Agreement. The recipient agency may copyright reports produced using data under this Agreement provided that the source agency shall have a royalty-free, non-exclusive, irrevocable right to publish, reproduce, distribute and use all or any part of said reports in any manner and for any purpose, without limitation, and may authorize others to do the same.

Under the terms of this Agreement, the recipient agency is not required to make reports or electronic files available to the public or a third party without an arrangement to recover costs associated with providing such reports or files. The recipient agency may charge for reasonable costs incurred to provide information to third parties pursuant to this Agreement.

**IX. DESTRUCTION OF RECORDS AND DATA**

Unless authorized by source agency to retain data, the recipient agency shall destroy all records and data, regardless of format, no later than sixty (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.

**X. SUSPENSION OR TERMINATION OF THIS AGREEMENT**

Upon sixty (60) days written notice, either party may suspend or terminate this Agreement without cause.

The source agency may suspend or terminate the Agreement immediately for cause under any of the following circumstances:

1. Use of information provided under this Agreement for an unauthorized purpose, as outlined in Article III;
2. Failure to comply with the requirements for receiving information as outlined in Article IV;
3. Failure to protect the confidentiality of information or to protect such information against unauthorized access or disclosure as outlined under Article V;
4. Unauthorized sharing of information under this Agreement with third parties, vendors, contractors, or subcontractors as outlined in Article VII:
5. Failure to obtain approval to release reports or files and provide copies of such reports or files as outlined in Article VIII;
6. Access to data or information in a manner or by staff not authorized to receive data or information as outlined in Appendix B.

The termination or suspension of the Agreement shall be effective immediately upon notification of the recipient agency. The source agency shall provide a written explanation of the termination or suspension within thirty (30) days after the notification to the recipient agency. The recipient agency shall cooperate with the source agency in investigations of individual staff violations and shall take appropriate actions against staff who commit violations of this Agreement.

Any suspension of this Agreement shall remain in effect until the source agency is satisfied that the recipient agency is in compliance with the terms of the Agreement. The source agency may also suspend or terminate the access of individual recipient agency staff to data under this Agreement without suspending or terminating the overall Agreement.

The penalties under state and federal law for violations of confidentiality requirements pertaining to Confidential Information or PII may apply to the recipient agency or individual recipient agency staff regardless of actions taken by the source agency to suspend or terminate the Agreement. Suspension or termination of the Agreement shall not preclude the source agency from seeking prosecution of individuals or other imposition of penalties on the recipient agency for confidentiality violations as provided under state or federal law.

The confidentiality and disclosure requirements of this Agreement survive the termination, for whatever reason, of the Agreement itself, subject to applicable state and federal laws.

**XI. AMENDMENT OF THIS AGREEMENT**

This Agreement may be amended at any time by written amendment signed by the signatories to this Agreement (see Article XIII) or their designees. Appendices to the Agreement may be amended at any time by written agreement of the Source Agency’s Data Steward(s) and the Recipient Agency’s Officials with Authority to Access or Grant Access (see Appendix A).

Each party agrees to give the other party written notice within thirty (30) days after becoming aware of any policy, procedure or technology changes which may impact upon the performance of either party under this Agreement.

This Agreement is subject to federal and state law, codes, and regulations, all of which are subject to change. Upon applicable federal or state law or regulation change, this Agreement shall be considered immediately modified in accordance with each such change, without notice or written amendment.

This provision for automatic amendment shall not apply where one party provides written notice to the other party within sixty (60) days after the effective date of the federal or state law or regulation change that it desires to amend the Agreement. Upon giving the required notice, the source and recipient agencies agree to negotiate the effect the particular federal or state law or regulation change will have on this Agreement.

If this Agreement conflicts with any future specific agreements between the source and recipient agencies, then that other specific agreement shall be the prevailing Agreement regarding only those specific parts of any such agreement that conflict with this Agreement.

**XII. OTHER ISSUES FOR AGREEMENT**

The source agency will make the recipient agency aware of changes to administrative data systems that will affect use of information shared and authorized by this Agreement.

**XIII. SIGNATURE BLOCK**

**For Source Agency:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (Print), Division Administrator, Division Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (Print), Deputy Secretary, Department of Children and Families Date

**For Recipient Agency:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (Print), Title Date

|  |
| --- |
| **APPENDIX A**DATA SHARING AGREEMENTBETWEENTHE DEPARTMENT OF CHILDREN AND FAMILIES (DCF)AND THE[Recipient agency name] |

**DCF Data Steward(s):**A DCF Data Steward is an individual designated by DCF, the source agency to:

* 1. Coordinate, administer and maintain amendments (attachments) to this Agreement.
	2. Coordinate requests between the source agency and the authorized individuals listed below to facilitate access of data, monitor recipient agency data sharing compliance, or request changes to this Agreement.

Only the following authorized individuals shall be able to act as a DCF Data Steward in accordance with the goals of this Agreement, and shall serve as the source agency’s contact persons for all purposes of this Agreement:

|  |  |  |
| --- | --- | --- |
| **Name/Title** | **Phone** | **Email** |
|  |  |  |
|  |  |  |

**Recipient Agency’s Officials with Authority to Grant Access:**

Only the following authorized individuals shall be able to establish users and grant access to information and/or data systems in accordance with the goals of this Agreement, and shall serve as the recipient agency’s contact persons for all purposes of this Agreement:

|  |  |  |
| --- | --- | --- |
| **Name/Title** | **Phone** | **Email** |
|  |  |  |
|  |  |  |
|  |  |  |

The recipient agency is expected to provide appropriate ongoing training and technical assistance for the above named individuals in support of the outcomes of this Data Sharing Agreement.

**Recipient Agency’ Officials with Authority to Access or Request Information** (Delete this section if only access to DCF data systems is given)**:**

Only the following authorized individuals shall be able to access information or data in accordance with the goals of this Agreement:

|  |  |  |
| --- | --- | --- |
| **Name/Title** | **Phone** | **Email** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **APPENDIX B**DATA SHARING AGREEMENTBETWEENTHE DEPARTMENT OF CHILDREN AND FAMILIES (DCF)AND THE[Recipient agency name] |

**Data and/or Access to be Provided:**

(Description of dataset, in as much detail as necessary to identify only essential data to be transported)

**Access: (Choose One, delete the other)**

**Format of the Data to be provided:**

Data shall be made available in the following format(s):

Limitations to access and data are as follows:

**Method of Accessing Data:**

Access to data or systems identified above shall be granted in the following way:

Requests for data or access should be directed to the DCF Data Steward designated in Appendix A to this Agreement.

**Other Specific Relevant Protocols, Guidelines, or Information:**

(Complete as necessary)