

**CHILD DEATH REVIEW CASE REPORTING SYSTEM
DATA USE AGREEMENT BETWEEN
THE MICHIGAN PUBLIC HEALTH INSTITUTE AND THE HEALTH DEPARTMENT
OF KITTITAS COUNTY**

This data use agreement is entered into on January 1, 2013 between the Michigan Public Health Institute (MPHI) (known hereafter as “Receiver”) and the Kittitas County Public Health Department (known hereafter as “Holder”) until terminated by either party.

The purpose of this agreement is to establish the terms and conditions for the collection, storage and use of data obtained from the case reviews of child deaths submitted by Child Death Review (CDR) teams in Kittitas County and entrusted to the Michigan Public Health Institute as the Child Death Review Case Reporting System (CDR-CRS).

A. The Receiver

1. The Michigan Public Health Institute is a non-profit private agency. It has a Cooperative Agreement, Number U49MC00225, with the Maternal and Child Health Bureau, Health Resources and Services Administration, U.S. Department of Health and Human Services, to manage the National Center for the Review and Prevention of Child Deaths (NCRPCD). As part of this agreement, MPHI is to manage a standardized, web-based reporting system for state and local child death review teams.
2. MPHI also manages the MPHI Management Information Technology program (MIT) and the Interactive Solutions Group (ISG).
3. The NCRPCD is responsible for the development of the CDR-CRS, training and liaison to state agencies participating in the system, technical assistance in using the system, and analysis and dissemination of national CDR data generated by the system. MIT and ISG are responsible for maintenance of the servers at MPHI, including firewall protection and other securities. ISG is responsible for data storage and data access by users of the CDR-CRS.
4. MPHI holds a Federal-wide Assurance (FWA) that is a written commitment to protect human research subjects by complying with federal regulations and maintaining adequate programs and procedures for the protection of human subjects. This FWA specifies adherence to the Code of Federal Regulations Title 45 Public Welfare Part 46 Protection of Human Subjects, and the use of the Belmont Report as an ethics guideline. The NCRPCD including the CDR-CRS is reviewed annually by the MPHI Institutional Review Board. Copies of the panel decision letters are available to the Holder.
5. MPHI complies with the federal privacy requirements specified in the HIPAA Privacy and Security Rules (45 CFR Parts 160, 162 and 164, Standards for Privacy of Individually Identifiable Health Information). The Institute has an appointed Privacy Officer and Privacy Panel, developed and adopted HIPAA-compliant privacy and security policies and procedures, and all staff receive training in these policies and procedures. MPHI's Institutional Review Board/Privacy Panel annually reviews the NCRPCD, including the CDR-CRS, for adherence to HIPAA regulations and MPHI policy. Copies of the panel decision letters are available to the Holder.

B. The Holder

The holder, Kittitas County Public Health Department, is the lead for the local CDR team pursuant to RCW 70.05.170 which authorizes local health departments to conduct child mortality reviews in Washington State.

C. Liaison: The Washington State Department of Health will serve as a liaison between the Holder and the Receiver in order to provide communication and oversee data requests for the CDR Case Reporting System. The Washington State Department of Health will have access to the identifiable data via the CDR Case Reporting System for the State of Washington.

D. Purpose of and Type of Data

1. The Kittitas County Public Health Department Child Death Review Team are supplying data to the (NCRPCD) in order to:
 - a. Provide the state and local CDR teams with a comprehensive CDR case reporting system for collecting, analyzing and reporting on their reviews of child deaths.
 - b. Permit comparability of CDR data within and between local CDR teams and states.
 - c. Use data collected to promote policy, programs, services and laws to prevent child deaths at the local, state and national levels.

E. Data Entry and Transmittal

1. Data is submitted by the Holder to the Receiver only via the Internet, using the CDR-CRS, ©Michigan Public Health Institute. The Receiver will provide paper forms to the Holder upon request, however all data is obtained by the Receiver through the Internet.
2. The Holder is complying with their applicable state laws and policies in making the determination on the specific data to be entered into this system and the persons they authorize to enter and transmit the data. Relevant Holder state CDR statutes or promulgated rules are provided in Appendix A.
3. Only persons selected by the Holder and provided with a password by the Holder or Receiver will have access to the CDR-CRS for data entry and submission as a data entry user.
4. The Receiver will create and administer data entry user accounts when the Holder makes requests, or accounts can be created and maintained by the assigned state administrators of this reporting system upon request of the Holder.
5. Accounts are locked out when a user fails to log in successfully 5 times in 10 minutes; such accounts remain locked out until released by NCRPCD staff or assigned state administrators.
6. Accounts are automatically logged out after 60 minutes when there is no transmission to the server, unless the Holder adjusts this time out expiration period via coordination with NCRPCD.
7. Both the Receiver and/or the Holder's assigned state administrator may terminate a user's access to the system at any time.

F. Data Storage

1. All data submitted via the Internet using the CDR-CRS is stored on a server located within the MPHI Data Center.
2. Data is stored on this server indefinitely unless the Holder terminates the data use agreement.
3. The Receiver ensures the security of these servers in the following ways:
 - a. Data transmitted to and from the web server are authenticated and encrypted with 256-bit SSL (Secured Sockets Layer), which is the strongest currently available commercially. The certificate authority is *GoDaddy* and is renewed annually.
 - b. A firewall is maintained to protect its web servers from unauthorized access via the Internet.
 - c. The servers are in a physically secure location with restricted access and a complete automatic temperature alarm system and fire sprinkler protection system. The server rooms have separate air conditioning systems, and electrical supplies are backed up with uninterruptible power supplies.
 - d. When the MPHI Data Center is closed during non-business hours, the building is locked, an electronic alarm system is activated and access into the building is permitted only through the use of electronic reader cards. The MPHI Data Center is also equipped with a video surveillance system.
 - e. MPHI continuously updates virus-scanning software on all servers and workstations.
 - f. A small group of MIT and ISG staff have access to the server room for server management and maintenance. These staff abide by strict confidentiality agreements. These individuals will be identified and their signed security agreements provided upon request of the Holder.
 - g. Custodial and building maintenance staff are not allowed in the server area except in the presence of MIT and ISG staff.
 - h. MIT and ISG staff regularly and randomly audit their database servers to ensure there are no security violations.
4. For disaster recovery MPHI network servers are backed-up nightly onto tape and the backups are delivered in locked containers via courier and stored off-site in a physically secure location. This location is a data warehouse with full exterior and interior security. These backups protect the data against unexpected loss due to fire, flood or damage to the network servers.
5. The Receiver is not responsible for any damage caused by viruses originating from any places not attributable to the Receiver.
6. It is strongly suggested that the Holder have consistent/comparable security practices in place for data that is downloaded from the servers back to the Holder or back to the Holder's identified users.

G. Access to the CDR Data on the Servers

1. MPHI staff managing the server and CDR-CRS will only access the data submitted by the Holder in the event that there are unforeseen problems with the database that need

- troubleshooting, correction or upgrading. MPHI staff will not amend, addend, alter or erase any information contained in data files without prior written authorization.
2. Identifiers will be removed from data downloads based on the permission levels for both the Holder and Receiver. This removal of data elements is a software program feature of the CDR-CRS.
 3. NCRPCD staff will have access only to data submitted by the Holder and their authorized data entry persons that have case identifiers removed using the HIPAA standards listed in Appendix B, unless in the event of unforeseen problems with the database that requires troubleshooting.
 4. The Holder will identify the level of access to data of their authorized persons at both the state and local level. Data will be accessible to the Holder via the Internet.
 5. The Holder will provide the Receiver with the written names and contact information for persons that will be able to access data in the event the Receiver is asked to create logins by the Holder.
 6. Any breach of security or unintended disclosure known by the Receiver will be reported immediately to the appropriate MPHI supervisors, Privacy Officer and IRB chair. The Holder will then be notified of this adverse event and steps will be taken in coordination with the Holder to mitigate harm and cure the breach of security within thirty days. As stated in Section A, the privacy protocols and policies in place at MPHI are in compliance with HIPAA and meet or exceed federal standards.
 7. Any breach of security or unintended disclosure known by the Holder will be reported immediately to the Receiver, and steps will be taken in coordination with the Holder to mitigate harm.

H. Permitted Data Uses

1. Data housed at MPHI is not subject to the Freedom of Information Act (FOIA) and, as such, no data submitted by the Holder will be released by MPHI in response to any FOIA request. The Holder will address any FOIA request made to the Holder.
2. All data accessed by and released to the Holder are the responsibility of the Holder. Any subsequent breaches of security or confidentiality once the Holder obtains the data are the responsibility of the Holder.
3. The Holder is complying with their applicable state laws and policies in making the determination on the specific data allowed to be disclosed by the Receiver.
4. The Receiver will not release any data that includes identifiable characteristics as defined by HIPAA (Appendix B) to any persons or organizations, except in the circumstances provided in writing by the Holder.
5. The Receiver may release de-identified data only in accordance with the MPHI IRB approved data dissemination policy (Appendix E).
6. All reports released by the Receiver and Holder shall be developed with adequate provision for the accuracy, reliability and integrity of the data.

I. Ownership


1. The Receiver acknowledges that all child death review data submitted by the Holder and the Holder's designated data entry persons shall be and remain the sole property of the Holder.
2. The Holder acknowledges that the CDR-CRS and all of its software platform applications are the copyrighted property of the Michigan Public Health Institute.

J. Agreement Terms and Termination

1. This agreement applies to all activities occurring between January 1, 2013 and December 31, 2015
2. This agreement may be terminated by the Holder or Receiver under the following circumstances:
 - a. If the Holder wishes to terminate their relationship with the Receiver for any reason.
 - b. If the Holder of data can no longer participate in the Internet web system due to changes in laws or funding for CDR programs.
 - c. If the Receiver of data no longer receives funding to serve as the NCRPCD.
3. Upon termination of this agreement, the Receiver, shall, upon request of the Holder, remove all of the Holder's child death review case data stored on the server. Child death review data stored on backup tapes cannot be removed in the event of the Holder's termination but will never be reported or disseminated by the Receiver.
4. Any subcontractors or other agents hired by the Receiver or Holder must agree to the same restrictions and conditions that apply through this agreement.
5. All Receiver staff with access to the data submitted by the Holder will sign a confidentiality agreement (Appendix C).
6. The Receiver agrees to maintain an insurance rider to provide additional liability insurance, beyond that normally required for MPHI programs.

IN WITNESS WHEREOF, the parties hereto execute this agreement as follows:

Michigan Public Health Institute
Data Receiver

By: 
Jeffrey R. Taylor, PhD
Executive Director

Michigan Public Health Institute
Date: 2/1/13

State of Washington, Kittitas County
Data Holder

By: 
Administrator, Kittitas County Public Health Department
Date: 1/18/13


1/29/13

Appendix A
Relevant State CDR Statutes or Promulgated Rules for the
Collection, Analysis and Distribution of CDR Data

Washington RCW 70.05.170 Child mortality review (Revised 2010).

(1)(a) The legislature finds that the mortality rate in Washington state among infants and children less than eighteen years of age is unacceptably high, and that such mortality may be preventable. The legislature further finds that, through the performance of child mortality reviews, preventable causes of child mortality can be identified and addressed, thereby reducing the infant and child mortality in Washington state.

(b) It is the intent of the legislature to encourage the performance of child death reviews by local health departments by providing necessary legal protections to the families of children whose deaths are studied, local health department officials and employees, and health care professionals participating in child mortality review committee activities.

(2) As used in this section, "child mortality review" means a process authorized by a local health department as such department is defined in RCW 70.05.010 for examining factors that contribute to deaths of children less than eighteen years of age. The process may include a systematic review of medical, clinical, and hospital records; home interviews of parents and caretakers of children who have died; analysis of individual case information; and review of this information by a team of professionals in order to identify modifiable medical, socioeconomic, public health, behavioral, administrative, educational, and environmental factors associated with each death.

(3) Local health departments are authorized to conduct child mortality reviews. In conducting such review, the following provisions shall apply:

(a) All health care information collected as part of a child mortality review is confidential, subject to the restrictions on disclosure provided for in chapter 70.02 RCW. When documents are collected as part of a child mortality review, the records may be used solely by local health departments for the purposes of the review;

(b) No identifying information related to the deceased child, the child's guardians, or anyone interviewed as part of the child mortality review may be disclosed. Any such information shall be redacted from any records produced as part of the review;

(c) Any witness statements or documents collected from witnesses, or summaries or analyses of those statements or records prepared exclusively for purposes of a child mortality review, are not subject to public disclosure, discovery, subpoena, or introduction into evidence in any administrative, civil, or criminal proceeding related to the death of a child reviewed. This provision does not restrict or limit the discovery or subpoena from a health care provider of records or documents maintained by such health care provider in the ordinary course of business, whether or not such records or documents may have been supplied to a local health department pursuant to this section. This provision shall not restrict or limit the discovery or subpoena of documents from such witnesses simply because a copy of a document was collected as part of a child mortality review;

(d) No local health department official or employee, and no members of technical committees established to perform case reviews of selected child deaths may be examined in any administrative, civil, or criminal proceeding as to the existence or contents of documents assembled, prepared, or maintained for purposes of a child mortality review.

(e) This section shall not be construed to prohibit or restrict any person from reporting suspected child abuse or neglect under chapter 26.44 RCW nor to limit access to or use of any records, documents, information, or testimony in any civil or criminal action arising out of any report made pursuant to chapter 26.44 RCW.

(4) The department shall assist local health departments to collect the reports of any child mortality reviews conducted by local health departments and assist with entering the reports into a database to the extent that the data is not protected under subsection (3) of this section. Notwithstanding subsection (3) of this section, the department shall respond to any requests for data from the database to the extent permitted for health care information under chapter 70.02 RCW. In addition, the department shall provide technical assistance to local health departments and child death review coordinators conducting child mortality reviews and encourage communication among child death review teams. The department shall conduct these activities using only federal and private funding.

(5) This section does not prevent a local health department from publishing statistical compilations and reports related to the child mortality review. Any portions of such compilations and reports that identify individual cases and sources of information must be redacted.

Appendix B

HIPAA Required Elements to De-Identify Case Data^{*}

These data elements will be removed for all persons accessing de-identified case data, per the Data Use Agreement. The source of these data elements is the National Center for Review and Prevention of Child Deaths' Case Reporting System: Case Report Tool.

Introduction: Case Definition

Case number
County of review
Review team number
Sequence of review
Death certificate number
Birth certificate number

Section A: Child Information

Child first name
Child middle name
Child last name
Child name: unknown
Date of birth: month, day, and year
Date of birth: unknown
Date of death: month and day
Date of death: unknown
Residential address: unknown
Residential address: street
Residential address: apartment
Residential address: city
Residential address: county
Residential address: zip

Section D: Incident Information

Date of incident
Date of incident: same
Date of incident: unknown
Time of incident
Time of incident: am or pm
Time of incident: unknown
Incident County

Section N: Form Completed By

The names and contact information will be removed.

^{*} Source: <http://www.hhs.gov/ocr/combinedregtext.pdf>, Section 164.514(b)(2)(i) of the rules.

Appendix C Holder Confidentiality Agreements

Sample Confidentiality Statement for State and Local Users of the *Child Death Review Case Reporting System*

By signing this Agreement, I agree to the following when I access any and all components of the *Child Death Review Case Reporting System*

1. I will comply with all laws, regulations, policies and procedures as set by the State of _____
2. I will safeguard the confidentiality of all confidential information to which I have access. I will not carelessly handle confidential information. I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as within the scope of my duties.
3. I will only access confidential information for which I have a need to know and I will use that information only as needed to perform my duties.
4. I will safeguard and will not disclose my user name and password unless authorized by the state administrator of the reporting system. I understand that my user name and password allows me to access confidential information for my team on the *Child Death Review Case Reporting System*. I understand that the State administrator may revoke my access to the data system if my responsibilities change. *
5. I will promptly report activities by any individual or entity that I suspect may compromise the availability, integrity, security, or privacy of confidential information.
6. I understand that the ownership in any confidential information referred to in this Agreement is defined by State statute.
7. I understand that violating applicable laws and regulations may lead to other legal penalties imposed by the judicial system.

Signature: _____ **Date:** _____

Print Name: _____

* If your state already has confidentiality statements in place, you might consider replacing this form with your own, but adding statement four from above.

Appendix D

MPHI Confidentiality Agreement

Confidentiality Agreement for Michigan Public Health Institute Staff Assigned to Privacy-Sensitive Projects

As described in the Michigan Public Health Institute (MPHI) Employee Handbook, all MPHI employees have the responsibility to maintain the accuracy, availability, completeness, and confidentiality of the business information, trade secrets, and individually identifiable data to which they have access. Due to the nature of its work, MPHI has access to, stores, uses, and discloses confidential data (including protected health information as defined by the HIPAA Privacy Rule). Any or all of the following factors may require that use and disclosure of these data be restricted in various ways:

1. Federal, tribal, state, and local laws and regulations. Examples include the HIPAA Privacy Rule that governs medical privacy, and the Common Rule that governs Institutional Review Boards and research with human subjects.
2. MPHI policies and procedures, including project-specific protocols.
3. Contractual agreements between MPHI and its project partners or clients.

MPHI employees assigned to work on privacy-sensitive projects must annually sign this agreement to demonstrate that they are aware of their obligations to protect the confidentiality and security of the data to which they have access.

By signing this Agreement, I agree to the following:

1. I will comply with all laws, regulations, contractual agreements, MPHI policies and procedures, and project-specific protocols related to my assigned duties. I understand that I may be required to complete additional training related to these obligations.
2. I will safeguard and will not disclose my password(s), access code(s), or any other authorization(s) I have that allow me to access confidential information. I understand that MPHI may at any time revoke my password(s), access code(s), other authorization, or access to confidential information.
3. At all times during my employment, I will safeguard the confidentiality of all confidential information to which I have access. I will not carelessly handle confidential information. I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as properly authorized within the scope of my assigned duties at MPHI.
4. I will only access confidential information for which I have a need to know and I will use that information only as needed to perform my legitimate duties as an employee of MPHI. I will not misuse confidential information.
5. I will promptly report activities by any individual or entity that I suspect may compromise the availability, integrity, security, or privacy of confidential information held by MPHI. I understand that reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.
6. I understand that I have no right or ownership interest in any confidential information referred to in this Agreement.

7. I understand that my failure to comply with this Agreement may result in disciplinary action up to and including termination of my employment. I understand that violating applicable laws and regulations may lead to other legal penalties imposed by the judicial system, such as fines and/or imprisonment.
8. I understand and accept that signing this Agreement is a condition of my employment and that my obligations under this Agreement will continue after termination of my employment.

Employee Signature: _____ **Date:** _____

Print Employee Name: _____

Supervisor Signature: _____ **Date:** _____

Print Supervisor Name: _____

Appendix E
NCRPCD Data Dissemination Policy &
Guidelines for Requesting De-Identified Data Set

DATA DISSEMINATION POLICY

Mission

The purpose of the Child Death Review (CDR) Case Reporting System of the National Center for the Review and Prevention of Child Deaths (NCRPCD) is to systematically collect, analyze, and report on information surrounding deaths of individual children around the country. The information can then be used at the local, state, and national levels to inform improvement in child health and safety and to prevent deaths. The data collected with the System includes the following:

- information about the child, family, supervisor and perpetrator;
- the types of action taken during the investigation;
- the scene, incident, and background information on the cause of death, including the risk and protective factors;
- the services provided or needed as a result of the death;
- a descriptions of the teams' recommendations, as well as the policies, practices, and other actions taken to prevent other child deaths; and
- the factors affecting the quality of the case review.

The web-based CDR Case Reporting System was first implemented in May 2004 in 14 pilot states. Version 1 was made available for widespread use in January 2007, and Version 2 was released in January 2008. Prior to releasing any data, please obtain updated information on the number of participating states, number of entered cases and number of cases migrated into the system from older state reporting systems. The CDR Case Reporting System is supported by the U.S. Maternal and Child Health Bureau and resides on servers at the Michigan Public Health Institute (MPHI). There is no fee to states to use the System.

Data Sources

Data collected by the CDR Case Reporting System are the result of multi-disciplinary processes that bring together state and/or community agencies to share information on child death events and to identify the risk factors in these deaths. Data entered into the System may include, but is not limited to, information gathered from the following data sources: birth certificates, death certificates, law enforcement records, medical records, autopsy reports, child protective services reports, and Emergency Medical Services run reports.

Child Death Review Programs in States

Child death review programs vary by state with respect to the types of death reviewed (all deaths, non-natural deaths, all injuries, abuse and neglect, near-death, etc.); the maximum age of children whose deaths are reviewed (0-14, 0-17, 0-25, etc.); and the average time between review and death (ranges from 1 to 36 months). Due to these variances, the data are not universally consistent from state to state.

Because most states do not review or enter every child fatality into the System, the CDR Case Reporting System should not be directly compared with vital statistics data nor should it be used to compute incidence rates. All of these distinctions among states and limitations should be accounted for and noted in any analysis of the data. More information about child death review programs and selection of cases by states for review can be found at www.childdeathreview.org.

Data Ownership

Child death review data entered into the System is owned by the individual state that entered it (per the data use agreement executed with each state and MPH). Requests for de-identified, individual case report data will be submitted to the NCRPCD Data Review Committee, per guidelines contained in this document. NCRPCD will inform states participating in the CDR Case Reporting System of all approved applications. For any research request that proposes to identify data by state in any published or publicly released analysis or results, states will be provided an opportunity to have their state's data excluded from the study.

Removal of Identifiable Data Elements for Data Set

No data file that includes HIPAA-defined personally identifiable elements is available to researchers. The complete Case Report tool contains more than 275 questions (approximately 1,800 data variables) about an individual fatality. (The Case Report form can be viewed and downloaded at www.childdeathreview.org.) Although states often enter HIPPA-defined personally identifiable data elements (child's name, address, date of birth, date of death, date and time of incident, and incident county) into the System, all personally identifiable data elements are removed from any data file made available to researchers. The data variables that will be removed from the data file are listed in Attachment 1 of the Application for Access to De-identified Data Set (Application for Data). The "Narrative" field contained in Section M of the Case Report form will only be released to researchers under special circumstances.

Permitted Data Uses

The NCRPCD may release aggregated, de-identified data identified by state to requested parties without state permission. The NCRPCD will only report aggregated data with cell counts of 6 or more cases. Requests for de-identified data sets will only be released following guidelines contained in this document.

Data Quality

In order to standardize the collection and interpretation of data elements, the CDR Case Reporting System contains a comprehensive Data Dictionary that is readily available online when entering cases into the System or as a standalone PDF document that can be used by child death review teams during review meetings. Additionally, NCRPCD is readily available to provide technical assistance about the Case Report tool and is in constant communication with states about data and reporting questions. Since the data is owned by the individual participating states, states are responsible for cleaning data records, and states vary in the degree to which they review data for inconsistencies, incompleteness, or inaccuracies. NCRPCD has found that data quality appears to improve with increased time and training on the System. The Case Report tool contains by design some subjective questions to engage team discussion (e.g., "Was the death preventable?" or "Did an act of omission contribute to the death?"). The subjective nature

of some of the questions can, however, make data analysis more problematic. Finally, although teams record in the System which agencies participated in the child death review, the primary data source for each data element is not collected as part of the Case Report tool. If there is a discrepancy in information shared by the different agencies at the review meeting, it is up to the CDR teams to determine the best answer and there is no set primacy rule for data sources.

More information about the CDR Case Reporting System can be found in the February 2011 Supplement to the *Journal for Injury Prevention*.

GUIDELINES FOR REQUESTING DE-IDENTIFIED DATA SET

The Receiving Institution must be an institution of higher education, research organization, or government agency that employs the Investigator. The institution must be registered with the U.S. Office for Human Research Protections. If the institution is not registered, NCRPCD may permit access to institutions with a demonstrated record of using sensitive data according to commonly-accepted standards of research ethics. An authorized representative of the Receiving Institution must sign the Contract for Data.

An Application for Access to and Use of Data (Application for Data) must identify a principal investigator. The Investigator serves as the primary point of contact for all communications involving the Contract for Access to and Use of Data (Contract for Data). The Investigator must hold a faculty appointment or research position at the Receiving Institution (see definition below) and must sign the Contract for Data, by which the Investigator assumes responsibility for compliance with all terms of the Contract for Data by employees of the Receiving Institutions, including the day-to-day security of the electronic data and all printed output derived from the files.

Each additional researcher who will have access to the data must be identified on the Application for Data and must sign a Confidentiality Agreement for Use of Data (Attachment 3). The applicants will not release or permit others to release the dataset or any part of it to any persons other than those identified on the Application for Data.

Access to data is also subject to the following requirements:

- The researchers given access to the Center's data may not conduct analyses using the data other than those described in the Application for Data.
- The Investigator must obtain IRB approval for the final use of data to ensure appropriate usage.
- All data shared is and shall at all times remain the sole property of the state and local county teams which performed the child death reviews that are the source of the data. States have the right of first refusal to participate in this research project if the Investigator plans to publish or publicly release any analysis or results that identifies individual state.
- The researchers will not attempt nor permit others to attempt to use the dataset to learn the identity of any decedent. If the identity of a decedent should be inadvertently discovered by the investigator or any other researcher, the Investigator will make no use of this knowledge, will not permit others to use the knowledge, will not inform anyone else of this knowledge, and will inform NCRPCD of the discovery so it can prevent future discoveries.
- The data will only be reported at an aggregated level and no data will be released that identifies data by state jurisdiction without the explicit approval of the state(s).
- Only aggregated data with cell counts of 6 or more cases will be reported.
- All oral and written presentations or other distribution of information resulting from the use of this data shall be developed with adequate provision for the accuracy, reliability and integrity of the data.

- All oral and written presentations or other distribution of information resulting from the use of the requested data will be submitted to NCRPCD for review at least two weeks prior to presentation or submission to a journal or other source of publication as a quality assurance measure to assure that materials adhere to the application guidance. All such presentations or other distribution resulting from use of the requested data will include an acknowledgement of the participating states and NCRPCD. Any additional or other use of these data will be considered a breach of the Contract for Data, unless agreed upon in writing by both parties beforehand.
- When the proposed analyses are completed, all hard copies of the data will be destroyed with a cross-cut shredder or returned to NCRPCD upon completion of project within three years and all electronic data destroyed/deleted. Written confirmation that the data have been destroyed is required.
- All installations of the data must have electronic security measures in place to prevent unauthorized access, by electronic or physical means, to the confidential data provided or output from that data.

Data Quality

Only cases that have been identified and approved by the states as being complete and clean will be included in the de-identified data set. The NCRPCD will survey states on an annual basis to make this determination.

Application Process

To request a de-identified dataset from the NCRPCD Case Reporting System, the Investigator must complete the Application for Access to De-identified Data Set and must submit a detailed proposal to NCRPCD describing the purpose of the data request, methods for study, and mechanisms that will be used to keep the data secure (see Application form). Upon receipt, a review committee (consisting of representatives of participating states and members of the NCRPCD National Center Steering Committee) will evaluate the application on the basis of the following criteria:

- Quality of the research question(s) and objectives for use of the data;
- Whether the data elements requested are clearly described and whether access to those elements is necessary for the research questions;
- Qualifications of researchers who will have access to data;
- Sufficiency of safeguards in place to maintain the data security, confidentiality, and prevent unauthorized access to data;
- Extent to which the proposal is in accordance with the mission of Child Death Review, which is to better understand how and why children die and use the findings to take action that can prevent other deaths and improve the health and safety of children;
- Whether NCRPCD plans to conduct similar research, and
- Whether anticipated presentations, publications, or other dissemination of results from the research is consistent with the NCRPCD mission.

At a minimum, the committee will review applications on a quarterly basis. All applicants will be notified in writing by NCRPCD of the review committee's decision. After approval by the review committee, NCRPCD will inform the states participating in the CDR Case Reporting

System of the committee's decision. For any research request that proposes to identify data by state in any published or publicly released analysis or results, states will be provided an opportunity to have their state's data excluded from the study (Attachment 2).

There may be a fee associated with requests that are complex in nature, to be negotiated prior to final approval for access to the data. Typically, there will be no costs to researchers for access to the CDR Case Reporting System de-identified data set. Requests for more information about the data file and the process for gaining access to it should be directed to:

National Center for the Review and Prevention of Child Deaths
2455 Woodlake Circle
Okemos, MI 48864
Phone : (800) 656-2434
Fax : (517) 324-7365
Email : info@childdeathreview.org

**NATIONAL CENTER FOR THE REVIEW AND PREVENTION OF CHILD DEATHS
CASE REPORTING SYSTEM**

Application for De-identified Data Set

Please complete information other than signatures electronically.

For what year or years of the NCRPCD Case Reporting System are data requested?

2005 ____
2006 ____
2007 ____
2008 ____
2009 ____
2010 ____
2011 ____

Note: States have different timeframes for when cases are reviewed and entered into the CDR Case Reporting System. Only cases that have been identified and approved by the states as being complete and clean will be included in the de-identified data set. The NCRPCD will survey states on an annual basis to make this determination.

Cases migrated from previous child death review reporting systems into the CDR Case Reporting System will not be included in a standard dataset, but may be provided upon further consultation between the researcher and NCRPCD.

I. Investigator/researchers

Identify the Investigator who will carry out the Investigator duties described in the Guidelines and provide his/her curriculum vitae:

Name:
Title:
Institution:
Department:
Street address:
City:
State:
Zip:
Phone:
Email address:

Identify additional researchers/collaborators who will have access to the data and provide their curriculum vitae:

Name:
Title:

Institution:
 Department:
 Street address:
 City:
 State:
 Zip:
 Phone:
 Email address:

II. Use of NCRPCD Data

Provide a detailed study protocol that includes the following:

- A. Research question(s) and objectives for use of the data;
- B. Rationale for data use;
- C. Funding source;
- D. Methods for processing the data;
- E. List of variables needed to carry out the study using the Case Report form as the guide.
- F. Analysis that will be conducted (including software that will be used);
- G. Study timeframe;
- H. Anticipated presentations, publications, or dissemination of results.

III. Data Security

1. All users of the NCRPCD data must have electronic security measures in place to prevent access to the confidential data from unauthorized individuals. In the table below, provide a comprehensive list of all devices on which the data will be installed and indicate the electronic security measures that will be applied to each device.

For those devices that have access to the Internet, all four of the electronic security measures must be in place for this data request to be approved. For non-Internet devices, firewall protection is not required.

ID	Device type Indicate workstation, laptop, server, portable media, or other device	Internet enabled? Does the device have access to the Internet?(Y/N)	Electronic security measures			
			Password login The device requires a login ID and password at startup and after a period	Restricted directory access The directories containing the data are restricted	Virus protection Anti-virus software is installed on the device. (Y/N)	Firewall protection Fire technology is in place for devices that are connected

			of inactivity. (Y/N)	to authorized users who have logged in to the device (Y/N)		to the Internet (Y/N)
1						
2						
3						
4						

2. In addition to electronic security, the devices on which the data have been copied must be physically secured to prevent theft of the device. Describe below the physical security measure in place for each device.

ID	Location of the Device Indicate building name and office number	Description of physical security Examples are offices are locked when unoccupied; storage in secure cabinets when the device is not in use, and monitored access to the building where the data is stored.
1		
2		
3		
4		

IV. Registration Status of the Receiving Institution's Institutional Review Board

1. Identify the Receiving Institution, as that term is described in the Guidelines:

2. Does the Receiving Institution have an Institutional Review Board that is registered with the U.S. Office for Human Research Protections? ____ Yes ____ No

3. If the Institution does not have an IRB assurance number, answer the following questions. Skip this section if you responded "yes" to the previous question.

Describe your Institution in detail. What kind of work does it do? Include the type of organization, its profit/non-profit status, and primary sources of revenue.

What experience does the Institution have in overseeing the use of sensitive research data by its staff? Please give specific examples.

V. Confidentiality Agreement

Any researcher with access to the NCRPCD data must sign and return a Confidentiality Agreement (Attachment 3).

Contract for Access to and Use of Data

This contract specifies the conditions for release of National Center for the Review and Prevention of Child Deaths CDR Case Reporting System data, research, and reports for legitimate public health or related research. The intent of this contract is to foster such research and to prevent misrepresentation of the data.

This Contract for Access to and Use of Data (Contract for Use) is between _____ [Receiving Institution] and _____ Investigator] as principal investigator on the proposed analysis of the requested data (Applicants), and Michigan Public Health Institute/Center for the Review and Prevention of Child Deaths (NCRPCD).

Applicants agree to the following requirements for the use of the data and assure compliance with the requirements.

1. This agreement applies to all activities occurring between [insert dates].
2. No one will be permitted to use this data to conduct analyses other than those described in the Application for Access to and Use of Data that accompanies this statement.
3. IRB approval will be obtained for the final use of data to ensure appropriate usage.
4. All data shared is and shall at all times remain the sole property of the state and local teams which performed the child death reviews that are the source of the data.
5. NCRPCD will seek permission from the participating states for release of the data for the project described in the Application for Access to and Use of Data (Application for Data) if said states are to be named in the analysis or results. States have the right of first refusal to participate in this research project if applicant intends to identify state jurisdiction in any published or publicly released analysis or results.
6. Neither the dataset nor any part of it will be released to any persons other than those identified on the Application Data.
7. Applicants and all other researchers with access to the data will not attempt to use the dataset to learn the identity of any decedent. If the identity of a decedent should be inadvertently discovered, Applicants will make no use of this knowledge, nor will they permit others to use the knowledge. Applicants will inform NCRPCD of the discovery so it can prevent future discoveries. Applicants will not inform anyone else of the discovery of identity.
8. Applicants understand that not all deaths of children in the states have been reviewed by child death review teams and that not every child death review team in the country participates in the CDR Case Reporting System.

9. Applicants understand that data will only be reported at an aggregated level and no data will be released that identifies data by state jurisdiction without explicit state permission. Aggregated data must have cell counts of 6 or more cases in order to be reported.
10. All oral and written presentations or other distribution of information resulting from the use of this data shall be developed with adequate provision for the accuracy, reliability and integrity of the data.
11. All oral and written presentations or other distribution of information resulting from the use of the requested data will be submitted to the NCRPCD for review at least two weeks prior to presentation or submission to a journal or other source of publication as a quality assurance measure to assure that materials adhere to the application guidance.
12. All oral and written presentations or other distribution of information resulting from use of the requested data will include an acknowledgement of the participating states and NCRPCD.
13. The sharing of this data does not imply, in whole or in part, that the proposed topic has not been investigated before, or will not be investigated now or in the future, by other investigators interested in this topic.
14. Any additional or other use of these data except as described in Applicants' Application Data will be considered a breach of this contract, unless agreed upon in writing by both parties beforehand.
15. Applicants will assure compliance with the security measures described in the Application Data.
16. When the proposed analyses are completed, all copies of the data will be destroyed with a cross-cut shredder or returned to the NCRPCD upon completion of project plus three years. All electronic versions of the data will be deleted. Written confirmation that the data have been destroyed/deleted is required.
17. By signing this document Applicants agree to be responsible for compliance with the conditions of this agreement and agrees to these conditions by their signatures below.
18. The fee for obtaining the data file is: _____, to be paid to the Michigan Public Health Institute, within 30 days of receipt of the data.

Investigator:

Name: _____ Title: _____

Organization: _____

Address: _____

Email address: _____ Phone: (____) _____

Signature: _____ Date: _____

For Receiving Institution:

Name: _____ Title: _____

Organization: _____

Address: _____

Email address: _____ Phone: (____) _____

Signature: _____ Date: _____

MPHI Executive Director:

Name: _____ Title: _____

Organization: _____

Address: _____

Email address: _____ Phone: (____) _____

Signature: _____ Date: _____

Attachment 1 HIPAA Required Elements to De-Identify Case Data *

These data elements will be removed for all persons accessing de-identified case data, per the Data Use Agreement. The source of these data elements is the National Center for Child Death Review Case Reporting System: Case Report Tool.

Introduction: Case Definition

Case number
County of review
Review team number
Sequence of review
Death certificate number
Birth certificate number

Section A: Child Information

Child first name
Child middle name
Child last name
Child name: unknown
Date of birth: month, day, year
Date of birth: unknown
Date of death: month and day
Date of death: unknown
Residential address: unknown
Residential address: street
Residential address: apartment
Residential address: city
Residential address: county
Residential address: zip

Section D: Incident Information

Date of incident
Date of incident: same
Date of incident: unknown
Time of incident
Time of incident: am or pm
Time of incident: unknown
Incident County

Section M: Narrative

The entire narrative will be removed

Section N: Form Completed By

The names and contact information will be removed.

* * Source: <http://www.hhs.gov/ocr/combinedregtext.pdf>, Section 164.514(b)(2)(i) of the rules.

Attachment 2

A Request for the Release of CDR Case Report Data when Research Applicant Intends to Identify State(s) in Proposed Published Analysis or Results

The following template will be used to request written authorization from states participating with the CDR Case Reporting System for permission to release individual case report data for research applicants that intend to identify state jurisdiction in published analysis or results. State permission will be sought once the application committee has determined the project has successfully met all review criteria.

Dear State of (insert state) Data Holder:

This letter is to inform you that the National Center for Review and Prevention of Child Deaths (NCRPCD) has received a request to release de-identified individual cases report data. The request was submitted by (insert name of requestor and organization) on (insert date).

The requester will be using the data for the purpose of (insert purpose). If the user intends to use the data for a purpose other than what is stated here, they must submit a new request.

Per the National Center for the Review and Prevention of Child Deaths' Guidelines for Requesting De-identified Data Set, written permission is necessary from each state where the research applicant intends to identify state jurisdictions in published or publicly released analysis or results of CDR data.

As a reminder, de-identified individual case report data released by the NCRPCD will not include the list of data elements found in Appendix B of the data use agreement.

Please verify that your state is not precluded from releasing this data by any rules or statutes before signing this agreement.

If you approve this data request, please sign both copies of this request letter. Keep one copy for your records and mail the other copy to the National Center for Review and Prevention of Child Deaths.

State of (insert state)
Data Holder

By: _____

(Signature of person with authority to sign agreement for the holder of data)

Date: _____

Attachment 3
Confidentiality Agreement to be signed by all Researchers with Access to NCRPCD Data

By signing this Agreement, I agree to the following:

1. I will safeguard the confidentiality of all confidential information contained in the National CDR data set to which I have been given access. I will not carelessly handle confidential information. I will not in any way divulge, copy, release, sell, loan, review, or alter any confidential information except as within the scope of my duties.
2. I will only access confidential information for which I have a need to know and I will use that information only as needed to perform my duties.
3. I will transmit and store all electronic and hard copy data in a secure and confidential manner and location at all times.
4. Upon completion of the performance of my duties the identifiable data set will be destroyed and no opportunities will be available to access that data on the network or computer systems.
5. I will promptly report activities by any individual or entity that I suspect may compromise the availability, integrity, security, or privacy of confidential information.
6. I understand that the ownership in any confidential information referred to in this Agreement is defined by State statutes.
7. I understand that violating applicable laws and regulations may lead to other legal penalties imposed by the judicial system.

Signature: _____ **Date:** _____

Print Name: _____