****

**MATERNAL MORTALITY REVIEW INFORMATION APPLICATION (MMRIA)**

**DATA SHARING AGREEMENT (DSA)**

**Between**

**[STATE/JURISDICTION]**

**And**

**MATERNAL MORTALITY PREVENTION TEAM**

**CENTERS FOR DISEASE CONTROL AND PREVENTION**

****

Version 0.8

June 15, 2022

Contents

[1. Purpose 1](#_Toc50066686)

[2. MMRIA System Overview 1](#_Toc50066687)

[3. Data Captured in MMRIA 1](#_Toc50066688)

[Personally Identifiable Information 2](#_Toc50066689)

[Data Ownership 2](#_Toc50066690)

[Privacy Act Applicability 2](#_Toc50066691)

[Data Integrity 2](#_Toc50066692)

[4. Secure Upload of Data 2](#_Toc50066693)

[5. CDC Management and Analyses of Shared Data 3](#_Toc50066694)

[6. Security and Confidentiality of Shared Data 3](#_Toc50066695)

[7. Data Breach Response 4](#_Toc50066696)

[8. Non-endorsement and Intellectual Property 5](#_Toc50066697)

[9. Liability 5](#_Toc50066698)

[10. Duration 5](#_Toc50066699)

[11. Resources 5](#_Toc50066700)

[12. Signatures 5](#_Toc50066701)

# Purpose

This document outlines the terms by which the jurisdiction[[1]](#footnote-1) of \_\_\_\_\_\_\_\_\_\_\_\_ will agree to share Maternal Mortality Review Committee (MMRC) data collected (described in Section 4) in their instance of CDC’s Maternal Mortality Review Information Application (MMRIA, or "Maria"). CDC requests jurisdiction data in order to improve data quality, identify technical assistance needs, and perform detailed analyses across MMRIA users regarding deaths that occur during pregnancy or in the year after the end of pregnancy.

A jurisdiction’s MMRIA data is not accessible to CDC staff for analysis purposes unless the jurisdiction specifically grants approval in writing. The “Maternal Mortality Review Information Application (MMRIA) Data Sharing Agreement (DSA)” constitutes that written approval and outlines the processes and information technology measures that CDC will employ to ensure protection of the confidentiality and security of all shared data.

# MMRIA System Overview

MMRIA is a consolidated data management system that enables jurisdiction based MMRCs to collect and analyze data regarding maternal deaths. The system facilitates the process of case review.

In order to comprehensively review each case of maternal death, MMRCs must capture detailed medical and social information on each woman who dies during pregnancy or within one year of the end of pregnancy in their jurisdiction. MMRCs employ abstractors within their jurisdictions who collect the pertinent information for each case by accessing medical records and social service records; death certificates; birth certificates for the index pregnancy, where applicable; and autopsy reports. The jurisdiction-based abstractors then manually enter relevant case details into MMRIA. The system produces a semi-automated case narrative that abstractors can then print and present to committee members to read during MMRC meetings, which convene on a routine basis as decided by the committee, typically monthly or quarterly. During or shortly after meetings, abstractors enter the committee’s findings on preventability, contributing factors, and recommendations to prevent future pregnancy-related deaths into MMRIA.

CDC is transitioning MMRIA users from local installations of the application to a centralized environment hosted at CDC. Each jurisdiction has access to and maintains their own independent installation of MMRIA in the CDC environment. CDC does not have access to a jurisdiction’s data unless it is explicitly shared with CDC. In rare cases, software support situations will require access to a jurisdiction’s data. CDC practices the principle of least privilege and has identified a limited number of individuals who may need to access MMRIA data for software support. Access is strictly limited to those individuals.

# Data Captured in MMRIA

Each case record may contain up to 1000 data elements. A full list of all data elements collected is currently available at <https://demo-mmria.cdc.gov/data-dictionary>

## Personally Identifiable Information

The following Personally Identifiable Information (PII) may be collected and maintained in MMRIA:

|  |  |  |
| --- | --- | --- |
| **Data pertaining to women who died during or within one year of end of pregnancy** | **Data pertaining to healthcare facilities** | **Data pertaining to MMRIA system users** |
| Name | Name | Name |
| Date of Birth | Address | Email address |
| Medical Notes |  |  |
| Medical Records Numbers |  |  |
| Address of Last Known Residence |  |  |
| Military Status |  |  |
| Employment Status |  |  |
| Date of Birth of infant(s) born of the index pregnancy of the deceased woman |  |  |

Jurisdictions can only view data they have entered into MMRIA. PII can only be viewed and edited by a limited set of users assigned the Abstractor user role within each Jurisdiction. PII in MMRIA is necessary for process management; jurisdiction-based abstractors produce a de-identified case narrative of events preceding each woman's death, which is then provided to committee members who review each case. Abstractors must be able to identify individual records by name in order to locate records and enter data accurately. Abstractors remove all PII before presenting a case to the committee. No PII is shared from MMRIA to any external systems without written approval from the jurisdiction or unless required by applicable law.

## Data Ownership

The data contained within MMRIA is not owned by CDC. Each jurisdiction retains ownership of the data they enter into MMRIA.

## Privacy Act Applicability

No Privacy Notice is required because the Privacy Act does not apply to deceased individuals.

## Data Integrity

The data contained within MMRIA is not owned by CDC. The jurisdiction is responsible for the integrity of the data shared. CDC will protect the integrity of all data shared by a jurisdiction.

# Secure Upload of Data

CDC employs Citrix ShareFile[[2]](#footnote-2) to provide a secure mechanism for partners to share data with CDC. CDC ShareFile enables a user to send a file securely to be downloaded via a secure hyperlink (“Send a File” feature) and to request that another user upload a file via a secure hyperlink (“Request a File” feature).

When a jurisdiction is ready to share a data file, they should first email or phone a MMRIA team point of contact. The MMRIA team will then use ShareFile to send a “Request a File” email to the jurisdiction containing a unique hyperlink that the state can click to begin the file upload process to MMRIA’s secure ShareFile space. For security purposes, each hyperlink will be configured to expire if it is not used within 48 hours. ShareFile hyperlinks are randomly generated to provide additional protection.

ShareFile utilizes Transport Layer Security (TLS) v 1.2 to ensure that payloads are protected in transit. TLS is a cryptographic protocol that enables secure communications over the internet. Depending on web browser capabilities, files are encrypted with up to a 256-bit encryption. Data at rest in ShareFile is encrypted using Advanced Encryption Standard (AES) with a 256-bit key.

Any web browser with access to the internet can be used to upload or download files with ShareFile. It is not necessary to configure network ports or install any software. However, officially supported browsers include the latest versions of Google Chrome, Microsoft Edge, and Mozilla Firefox. Microsoft Internet Explorer version 11 or later and Apple Safari version 10 or newer are also supported.

As part of historical and/or periodic vital records data migration, IT support staff on the CDC MMRIA team will assist jurisdictions in securely transferring data stored in local instances of MMRIA or in vital records files to each jurisdiction’s MMRIA instance on Central Hosting. To upload data, jurisdictions administrators can choose to utilize either CDC ShareFile or the secure jurisdiction folder located on the MMRIA Documentation & Reports Site (<https://cdcpartners.sharepoint.com/sites/NCCDPHP/MMRIA>). If a jurisdiction is unsure how to create a data file for sharing, the CDC MMRIA team can provide assistance with steps needed for creating the file.

# CDC Management and Analyses of Shared Data

Upon execution of this Agreement, CDC shall be permitted to export the jurisdictions data from within the MMRIA system utilizing the standard export de-identification option that contains potential PII information specified in Appendix A, and de-identifies MMRIA fields specified in Appendix B for the specific purposes set out in this Agreement. Data files are placed in a restricted directory behind CDC’s firewall that is currently only accessible to the minimum number of individuals necessary. The de-identified data are then placed in another restricted directory behind CDC’s firewall to allow other CDC MMRIA team members and their representatives to perform analysis on the data.

Examples of information products from these analyses may include presentations used during site visits and at meetings; briefs, reports, and manuscripts of learning from the aggregated data; and trainings for MMRIA users. Data will not be presented that is identifiable to an individual state.

# Security and Confidentiality of Shared Data

Data will be encrypted in transit and at rest following the National Institute of Standards and Technology’s Federal Information Processing Standard (FIPS 140-2) for Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module 2 are accepted by the Federal agencies for the protection of sensitive information.

To the extent CDC has custody and/or control of the data, CDC will maintain such information as confidential and/or proprietary to the full extent allowable under applicable law. The principle of least privilege will be applied to ensure that only individuals who have an absolute need to access the data will be granted access.   
  
An internal CDC contractor is “any person or entity employed by CDC” and subcontractors are included in “employed by CDC, an agent, contractor, or business associate….”. All aspects for data and system confidentiality and non-disclosure are covered by the U.S. Department of Health and Human Services (HHS) mandated annual electronic attestation that CDC staff and internal contractors are required to agree to.

All CDC staff and internal contractors are required to annually attest to the “HHS Rules of Behavior (ROB) for the Use of HHS Information and IT Resources Policy”. The HHS ROBs include additional privacy and confidentiality clauses to address protecting data from misuse or disclosure at rest and while in transit. All users are strictly bound by these standard ROB, which covers numerous IT staff who are constantly being transitioned/on-boarded to handle data on multiple projects nationally.

All CDC system users are also required to review and sign additional stringent confidentiality/non-disclosure rules once a year as part of Annual IT Security Awareness Training. Penalties for violations include dismissal from service, fines, prosecution and/or imprisonment.

# Data Breach Response

The Office of Management and Budget (OMB) defines a breach as:

“The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for another than authorized purpose.”[[3]](#footnote-3)

If a breach of MMRIA data is suspected, CDC will work with the jurisdiction where the breach occurred to conduct an initial assessment to determine the type of data compromised, the number of records impacted, and the potential impact to CDC or the jurisdiction.

If a breach involving PII is discovered, CDC and/or the jurisdiction should be notified as soon as the breach is discovered. Next steps will follow the U.S. Department of Health and Human Services’ (HHS) “Policy for Preparing for and Responding to a Breach of Personally Identifiable Information (PII).“[[4]](#footnote-4)

# Non-endorsement and Intellectual Property

By entering into this DSA, CDC does not directly or indirectly endorse any particular organization, product, or service, whether directly or indirectly related to this DSA.

This DSA does not and is not intended to transfer to any of the Parties any rights in any intellectual property of another Party.

# Liability

Each Party will be responsible for its own acts and the results thereof and shall not be responsible for the acts of the other Parties and the results thereof.

# Duration

This DSA is entered into voluntarily by all Parties and may be terminated by any Party with thirty (30) days advance written notice to the other Party. Should parties terminate, CDC shall extend the protections and limitations set forth in the Agreement to the extent permitted by federal law.

# Resources

CDC’s activities as described herein are subject to the availability of appropriations and government resources.

# Signatures

The undersigned concur with this Data Sharing Agreement.

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

|  |  |  |
| --- | --- | --- |
| [Name and Credentials]  [Title]  [Agency/Organization] | Date | David Goodman, M.S., Ph.D. Date  Team Lead, Maternal Mortality Team  Division of Reproductive Health  Centers for Disease Control and  Prevention |

1. “Jurisdiction” refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees. [↑](#footnote-ref-1)
2. Citrix ShareFile Security FAQs <https://www.sharefile.com/resources/citrix-sharefile-security-and-compliance-frequently-asked-questions>. [↑](#footnote-ref-2)
3. OMB M-17-12 – *Preparing for and Responding to a Breach of Personally Identifiable Information (January 2017), page 9,* <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf> [↑](#footnote-ref-3)
4. Policy for Preparing for and Responding to a Breach of Personally Identifiable Information (PII), <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-preparing-and-responding-breach.html> [↑](#footnote-ref-4)