Contents

Purpose

This document outlines the terms by which the state/jurisdiction of _____ will utilize the CDC's Maternal Mortality Review Information Application (MMRIA) to collect and analyze data regarding maternal deaths.

System Overview

The Maternal Mortality Review Information Application (MMRIA, or "Maria") is a consolidated data management system that enables jurisdiction-based* Maternal Mortality Review Committees (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 for action into MMRIA.

Data from MMRIA is used in jurisdiction-based surveillance, monitoring and development of evidence-informed responses to prevent maternal deaths.

Transition to CDC Hosting

From April 2017 through February 2019, MMRIA was only available to jurisdictions to host on their own servers. This model of "local hosting" created a burden for jurisdictions' IT departments and required extensive technical support from the CDC-based MMRIA team. The transition to CDC hosting will ease the burden both on jurisdictions and the CDC-based MMRIA team. The subsequent sections of this document refer to CDC-hosted MMRIA.

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 demo.mmria.org/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

*jurisdiction refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees.

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.

Privacy Act

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

Data Security and Confidentiality

MMRIA is hosted on a CDC Cloud Services solution. As a cloud service, it is subject to full security assessment, authorization, and continuous monitoring under the Federal Risk and Authorization Management Program (FedRAMP). MMRIA will be secured for confidentiality and integrity at a moderate level based on the requirements of the Federal Information Security Management Act (FISMA).

MMRIA data is protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction—whether accidental or intentional—in order to maintain confidentiality, integrity, and availability. The security and privacy controls that provide this protection meet minimum federal requirements with additional risk-based and business-driven control implementation achieved through a defense-in-depth security structure.

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.

Per FedRAMP requirements, MMRIA employs more than 300 security controls. More information on the required FedRAMP security controls for systems deemed moderate can be found at https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

*jurisdiction refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees.

In addition to the extensive security controls in place, there are access control measures that jurisdictions can implement to further protect the data. These security measures include the following:

- Users logged into MMRIA should log out before leaving their desk, even if just for a short break.
- MMRIA Jurisdiction Administrators should promptly delete user accounts for users who leave the program.
- MMRIA users should memorize their login information and never share it with anyone.
- Users must never share account passwords or allow other users to use their account credentials. Users are responsible for all activities occurring from the use of their account credentials.
- Annual review of user accounts and access roles

Most jurisdictions have requirements for the protection of jurisdiction data and responsible use of jurisdiction data systems. If not, CDC can make specific usage recommendations.

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 extend allowable under applicable law.

Data Retention

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

Data Breach

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

"…a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."[1]

If a breach of MMRIA data is suspected, CDC will work with the appropriate jurisdiction 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 CDC's "Standard for Responding to Breaches of Personally Identifiable Information."

[1] OMB M-17-12 – *Preparing for and Responding to a Breach of Personally Identifiable Information* https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

*jurisdiction refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees.

System Access

CDC provides MMRIA as a service to jurisdictions. Access to MMRIA shall be limited based on a least-privilege approach and a need-to-know basis. All data entered into MMRIA is accessible only to users who have been granted access by their jurisdiction's designated Jurisdiction Administrator.

SAMS

CDC's Secure Access Management Services (SAMS) allows users who are outside the CDC firewall to securely access CDC applications such as MMRIA. Each jurisdiction will assign one or more SAMS Activity Administrators who will be responsible for creating user accounts, deactivating accounts as needed, and for identity-proofing their users. This puts the security of MMRIA data in the jurisdiction's hands. Jurisdictions are responsible for ensuring that users access and use the system appropriately.

If a jurisdiction staff person has SAMS access for other CDC applications, they will use the same SAMS account for MMRIA.

Jurisdictions

Each jurisdiction is assigned a separate URL. Users only have access to their jurisdiction's URL.

User Roles

MMRIA employs role-based access to ensure the concept of "Least Privilege" is implemented and only those who need access will have access.

There are 3 MMRIA roles in use within each jurisdiction's MMRIA instance: Jurisdiction Administrator, Abstractor and Committee Member.

- Jurisdiction Administrator: has read/write access to users and jurisdiction. Activity Administrator is responsible for creating, maintaining, and deleting user accounts for Abstractors and Committee Members in their jurisdiction. *Note: this is a separate role from the SAMS Activity Administrator, but one person can have both SAMS Activity Administrator and MMRIA Jurisdiction Administrator roles.*
- Abstractor: has read/write access to the case database for cases within their assigned jurisdiction. An Abstractor has access to PII.
- Committee Member: has read access to a de-identified case database for cases within their assigned jurisdiction. The de-identified case database contains no PII.

CDC Access to MMRIA Data

MMRIA data is not accessible to CDC staff *for analysis purposes* unless the jurisdiction specifically grants approval in writing. Despite the best efforts of CDC, some *software support situations* will require access to a jurisdiction's data. CDC has identified only a few individuals who may need to access MMRIA data for software support; access is limited to those individuals.

Hardware and Software Requirements for MMRIA Use

In general, MMRIA requires a standard entry-level personal computer that is capable of running the latest version of the Google Chrome browser and has access to high-speed internet connection. MMRIA is developed for use in Chrome and will not function properly in Internet Explorer or other browsers. MMRIA does not require the installation of any software by the end user.

*jurisdiction refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees.

Non-endorsement and Intellectual Property

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

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

Future Potential Agreement

To the extent a jurisdiction agrees to share data with CDC, the parties will enter into a separate data use and confidentiality agreement.

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 MOU 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.

Resources

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

Approval

The undersigned concur with this Memorandum of Understanding.

_____	_____	_____	_____
[name and credentials] [agency/organization]	Date	David Goodman, M.S., Ph.D. Team Lead, Maternal Mortality Team Division of Reproductive Health Centers for Disease Control and Prevention	Date

*jurisdiction refers primarily to states but includes select metropolitan areas or other U.S. jurisdictions that convene Maternal Mortality Review Committees.