Contents

Security Policy Purpose

This policy provides guidance to ensure that data from the Department of Health and Human Services (DHHS) and Office of Child Support (OCS) remains secure and establishes the structure for ensuring confidentiality of the DHHS/OCS information. All persons requesting access to DHHS/OCS Client Information System and/or the MiChildSupport System must read through and sign this policy as part of the application for access to the systems. Signing this policy confirms the signor's understanding of the necessary procedures required to handle the systems data and ensure compliance with MSHDA and DHHS/OCS's security and confidentiality protocol.

Ensuring Confidentiality

Maintaining the confidentiality of DHHS/OCS data requires users of the database and data handlers to adhere to strict protocol. To ensure confidentiality users and data handlers agree that:

- Information disclosed from the DHHS/OCS database will only be used for the purposes defined in this policy below.
- Records retained for evidentiary purposes will be retained only to the extent and for the period required by law.
- Information will be restricted to the owners/agents (O/A) staff who requires that information in the office performance of their job or contract duties.
- No individual's information will be accessed in the database without prior written authorization on the Certification and Authorization to Release Information (MSHDA Mgmt. 801A) form. Authorization consent forms are valid for 15 months from applicant/resident signature date.
- All staff of O/A will be instructed as to the confidential nature of the information, the safeguards required to protect the information, and civil, criminal, and internal penalties for non-compliance with the confidentiality requirements pertaining to this information.
- O/A and its authorized representatives must not disclose data in any way that would violate the privacy of the individuals.

- O/A must promptly notify MSHDA Compliance Administrator in writing of any suspected abuse or misuse of information received under this agreement.

Penalties

DHHS/OCS data must not be disclosed to any third parties. Willful disclosure or inspection of DHHS/OCS data can result in civil and criminal penalties.

- Unauthorized disclosure – felony conviction and fine up to $5,000 or imprisonment up to five (5) years.
- Unauthorized inspection – misdemeanor penalty of up to $1,000 and/or one (1) year imprisonment.

Use of DHHS/OCS Information

The information contained in the DHHS/OCS data share may only be used for limited official purposes as described in this policy below. The data available from the DHHS/OCS database is listed on the Chart of MSHDA Data Elements (MSHDA Mgmt. 801B).

DHHS/OSC Data Share is considered UIV and can be used as third-party verification (TPV). Use these reports for applicable MSHDA and federal programs and the requirements of the Upfront Income Verification (UIV) Security Policy. Use of UIV is part of the initiative to reduce errors in calculations of income and the overall burden of verifying the income claimed by residents. Introduction of this new tool compels O/A to follow MSHDA policies and security to ensure that residents are treated in a fair and consistent manner.

Owner/Agent Responsibilities

The O/A will be responsible for the following actions in relation to this security policy. The O/A must:

- Use this data to facilitate the timeliness, accuracy, and efficiency of the MSHDA rental/assistance programs as required by both state and federal regulations.
- Use the information provided by the DHHS/OCS database to determine participant's rent share or eligibility by:
  - ✓ Verifying income information and ineligible recipients.
  - ✓ Maintain accurate records for the designated MSHDA program or service.
  - ✓ Recovering improper rental payments.
  - ✓ Prosecuting tenants who make false claims or fraudulent statements.
  - ✓ Providing MSHDA/HUD/IRS with mandated data requirements; and
  - ✓ Any other purpose allowed under existing programs and applicable state/federal law.

- Retain in the applicant/resident file the signed copy of the Certification and Authorization to Release Information (MSHDA Mgmt. 801A) form.
- Use the data provided by the DHHS/OSC database to confirm:
  - ✓ Applicants/residents are in compliance with designated eligibility criteria.
  - ✓ The tenant is in the DHHS/OSC database.
  - ✓ The tenant receives the following grants with the program effective date and grant amounts: State Supplemental Security Income (SSI), State Disability Assistance (SDA), and Refugee Assistance Program (RAP).
  - ✓ The tenant received Child Support Payments from OCS.
  - ✓ If the tenant receives the following grants with the program effective date, grant amount, and program end date: Family Independence Program (FIP).
  - ✓ The amount of the Food Assistance Program (FAP) that the applicant/resident receives.
  - ✓ The receipt of Medicaid (Yes or No only), if applicable;
  - ✓ Applicant/resident is sanctioned, what was the amount, dates, and reason for sanction.
  - ✓ The number of people that are on a grant, if applicable.
  - ✓ Whether childcare was paid to a provider and the amount paid.

  - ✓ The DHHS/OSC case number and caseworker name for contact concerning questions about tenant eligibility.
  - ✓ The receipt of Low-Income Home Energy Assistance Program (LIHEAP), if applicable.
  - ✓ The receipt of State Emergency Relief (SER), if applicable.
- Print the document from the DHHS/OSC data share, even if no data is returned, for each adult household member (18 years of age or older) living in each unit being certified (E.g. head of household, spouse, and co-head), where child support has been identified on the MSHDA Income and Asset Checklist.
- Use the DHHS/OCS data only for certification, auditing, compliance, and HUD required purposes.
- Ensure all users receive security training at the time of implementation and at least annually, thereafter.
- Ensure the O/A representatives (Designated Quality Coordinator, Key persons, and Data Handlers) have reviewed and signed this Data Share Security Policy.
- Provide MSHDA a copy of the signed written authorization upon request for validating audit trails and verifying that the correct procedures were followed.
- Detect, deter, and report improper disclosures, unauthorized access, or security breaches to the Designated Quality Coordinator (DQC) who will report as follows:
  - ➢ E-mail all pertinent documentation to MSHDACompli@michigan.gov, type "DHHS/OCS Data Share" in the subject line (preferred); OR
  - ➢ Mail to:
    MSHDA,
    DHHS/OCS Data Share Compliance Administrator,
    735 E Michigan,
    PO Box 30044,
    Lansing, MI 48909

- Designate secure areas for data review and storage.
- Restrict use of printers, copiers, facsimile machines, etc. in the area.
- Control access to areas containing DHHS/OCS information.
- Maintain a policy on how to secure computer systems and output.
- Users must retrieve all computer printouts as soon as they are generated so that DHHS/OCS data is not left unattended:
  - ➢ Do not print to a shared printer unless the user plans to immediately retrieve the printout.
  - ➢ Keep printouts in applicants/residents file in a secure area.
  - ➢ Printouts should not be transported from premises.
  - ➢ Lock computer/log off/exit the system when leaving a workstation or when finished for the day (Do NOT leave session open when not in use.).
  - ➢ Use a password-protected screensaver.

- Destroy DHHS/OCS information when the data is no longer needed and provide secure disposal of DHHS/OCS information:
  - ➢ Destroy as soon as prescribed by HUD's policies and procedures or MSHDA's compliance policies and procedures.
  - ➢ Burn/shred.
  - ➢ Keep log of destroyed data:
    - ✓ Date destroyed.
    - ✓ How destroyed.
    - ✓ By whom.

DHHS/OCS Reports

DHHS/OCS reports will be stored in the resident file for the term of residency and for three years after residency ends for applicable HUD/MSHDA programs. DHHS/OCS reports will be stored in the

resident file for the term of residency and for seven years after residency ends for the Low-Income Housing Tax Credit program (LIHTC).

The appropriate staff will make a note in the file any time a copy of the DHHS/OCS data is obtained by authorized persons. This includes copies provided to the applicant/resident, staff responsible for compliance monitoring, other internal staff, MSHDA, HUD, CAs, PBCA or OIG staff. Under no circumstances will the DHHS/OCS information be provided to anyone other than those noted in this policy.

Providing DHHS/OCS Reports to Auditors

Government Auditors - DHHS/OCS reports may also be used by Contract Administrators (CAs), Performance Based Contract Administrators (PBCAs), Traditional Contracts Administrators (TCAs), MSHDA staff for monitoring compliance with the recertification process; Independent Auditors (IPAs) auditing an O/A compliance with MSHDA's compliance requirements verifying income and the accuracy of rent/subsidy determinations; and the Office of Inspector General (OIG) for auditing purposes.

Independent Auditors (IPAs) are approved to view DHHS/OCS information, when hired by an O/A to perform the compliance audit of the property, for use in determining the owner's compliance with verifying income determining the accuracy/eligibility of rent/subsidy calculations.

Providing DHHS/OCS Printouts to Residents

If a resident requests a copy of their own DHHS/OCS printout, a copy may be produced. The staff person providing the copy will note that the printout is a copy provided to the resident upon request. This note will include the following:

- This is not an original, this is a copy provided to: (List Resident Name)
- On (Date)
- By (Key person's Name)
- Resident's initials _____

Accessing the Data Share

Owners /Agents must complete the following steps to gain access to the Data Share portal:

1. Designate a Quality Coordinator to oversee the security of employees accessing the database,
2. Designate Key Persons, who will have access and generate reports from the database,
3. Designate Data Handlers, who will use the reports to verify applicant and resident income,
4. Have all designated staff read this policy and sign a copy,
5. Have all designated staff perform Security Awareness Training at the website noted below and generate a certificate of completion,
6. Have the Designated Quality Coordinator and Key Persons complete and sign an Enrollment Profile/Security Agreement (MSHDA Mgmt. 1796b).
7. Submit a copy of all signed documents along with **a list of properties managed by O/A and which Key person and Data Handler(s) are active at each property**.

Annually the designated users must:

1. Perform the Security Awareness Training and provide an updated certificate of completion.
2. Verify an updated Certification and Authorization to Release Information form has been received from the resident prior to generating a new DHHS/OCS report.
3. Provide an updated list of properties managed by the O/A and which Key person and Data Handler(s) are active at each property.

Security Awareness Training

Users must complete the online security training annually to maintain their awareness and compliance with the security procedures. To meet this annual requirement, users must complete the online Cyber-Awareness Challenge (for Federal, DoD and IC Personnel), using the Federal Employee version. At the end of the training, users must print and sign the certificate. The certificate of completion must be kept on site and a copy provided to MSHDA at implementation and annually thereafter. The training can be found at: https://public.cyber.mil/training/cyber-awareness-challenge/.
Security awareness training is a crucial aspect of ensuring the security of the DHHS/OCS data share and data. Users and potential users must be aware of the importance of respecting the privacy of data, following the established procedures to maintain privacy and security, and notifying the DQC in the event of a security or privacy violation. Before granting access to the DHHS/OCS data share, each person must be trained in the security procedures in this policy.

Key Persons (Users) and Data Handlers

Key Persons - Access the data share for a management agent to generate file reports. These individuals must complete the Enrollment Profile/Security Agreement (MSHDA Mgmt. 1796b) form to access the data share. The Key person agrees to only use their own username and password to access the DHHS/OCS Data Share database and will not share his/her username and password with anyone else.

Data Handlers - Any person using or handling the data generated from the DHHS/OCS database.

Designated Quality Coordinator (DQC)

In addition to Key persons and Data Handlers each management agent must have an additional independent staff member that monitors the use of the DHHS/OCS data share information.

DQC will have the responsibility of ensuring compliance with the security policies and procedures outlined in this document. These responsibilities include:

- Maintaining and enforcing the security procedures.
- Keeping records of all the Key person(s) and Data Handler(s) that work for the O/A by property and monitoring security issues.
- Communicating security information and requirements to appropriate personnel, including coordinating and/or conducting security awareness training sessions.
- Conducting at least a semi-annual review of all user IDs issued to determine if the users still have a valid need to access the DHHS/OCS data share and taking necessary steps to ensure that access rights are revoked or modified as appropriate; and
- Reporting any evidence of unauthorized access or known security breaches to **MSHDA staff** and taking immediate action to address the impact of the breach, including but not limited to prompt notification to **MSHDA's Compliance Administrator** and/or DHHS/OCS.

Computer System Security Requirements

The O/A agrees to use antivirus software to limit data destruction or unintended transmission via virus, worms, Trojan horses, or other malicious means. Remote access by other computers other than those specifically authorized is prohibited.

Authorized users of DHHS/OCS data are directed to avoid leaving DHHS/OCS data displayed on their computer screens where unauthorized users may view the information. If an authorized user is viewing DHHS/OCS data and an unauthorized user approaches the work area, the authorized user will lessen the chance of inadvertent disclosure of DHHS/OCS data by logging out of the DHHS/OCS data share or minimizing or closing out the screen on which the DHHS/OCS data is being displayed.

Technical

Technical requirements that must be followed to ensure confidentiality are:

- Each key person must have a valid user ID and password.
- IDs and passwords **MUST NOT BE SHARED**;
- No one may access the system using another user identity.
- Access to data is restricted based on eligibility/assistance requirements for the property; and
- Users agree that their access and activity are monitored and audited to comply with this Data Share Security Policy.

Passwords, and Password Changes

DHHS/OCS data share passwords will be changed in accordance with MSHDA secure system requirements. Passwords will need to be changed every 90 days; users will be prompted 7 days in advance of the pending password change. Passwords must be at a minimum 8 characters, one capital letter, and one special character.

Termination of Access

DHHS/OCS data share access granted to an employee or authorized user will be revoked when access is no longer required or prior to termination of that employee or user to ensure data safety. Termination of DHHS/OCS data share access requires the O/A to submit the Enrollment Profiles/Security Agreement (MSHDA Mgmt. 1796b) form to MSHDA's Compliance Administrator. Refer to Use of DHHS/OCS Information – Owner/Agents Responsibilities for contact information.

Audit Process

At random dates the OCS Auditor will run a User Activity report to generate a sample of file queries to be audited by the MSHDA Gatekeeper. Any requests for data from the MSHDA Gatekeeper for audit review purposes must be provided timely by the DHHS/OCS data share users and/or the Designated Quality Coordinator in order to retain active access to the data share site.

Typical audit requests will include a list of user files accessed by the DHHS user and will request the Certification and Authorization to Release Information forms for each file accessed in the DHHS/OCS database for a specified audit period. The audit request will consist of who pulled the report, date and time pulled, and the last 4 digits of the social security number ran. (MSHDA suggests that electronic copies of the authorization form should be stored using this information.)

- O/A must provide MSHDA a copy of the signed written authorization upon request for validating audit trails and verifying that the correct procedures were followed.

Acknowledgement

By signing this form, I acknowledge that I have read and understand the O/A Security Policy for using the DHHS/OCS Data share. I agree to abide by this policy and to report any improper disclosure of information.

_____
Name (please print)

_____ _____
Signature Date

CC: Property File
MSHDA's Compliance Administrator