



OFFICIAL

Workforce Development Agency, State of Michigan (WDASOM)

Policy Issuance (PI): 13-25

E-mailed: 03/20/14 (pv)

Date: March 20, 2014

To: Michigan Works! Agency (MWA) Directors

From: Gary Clark, Director, Office of Talent Development Services
Workforce Development Agency, State of Michigan

Subject: Confidentiality Requirements for the Receipt and Utilization of Wage Record Data

SIGNED

References: Michigan Employment Security Act

What Safeguards and Security Requirements Apply to Disclosed Information 20 CFR 603.9

The Workforce Investment Act (WIA) of 1998

The Trade Adjustment Assistance (TAA) Act of 1974

The Wagner-Peyser Act

The Social Welfare Act of 1939

The Food Stamp Act of 1977

Programs Affected: All programs funded through the WDA

Background: In order to streamline the programmatic registration process, increase documentation accuracy and gain insight on the quality of education and training programs, the WDA has partnered with the Unemployment Insurance Agency (UIA) to allow the MWA system access to Wage Record data.



Workforce Development Agency, State of Michigan

Victor Office Center | 201 North Washington Square, 5th Floor | Lansing, Michigan 48913

michigan.gov/bwt | 517.335.5858 | TTY 888.605.6722

The WDASOM is an equal opportunity employer/program. Auxiliary aids, services and other reasonable accommodations are available upon request to individuals with disabilities.

This policy provides the required confidentiality agreement to be signed by MWA Directors to authorize the sharing of this type of information.

Policy: The MWA Director must sign the attached Confidentiality Agreement on behalf of the staff for their MWA. This agreement attests that the confidential information supplied by the UIA will be used only for the purpose stated in the separate Memorandum of Understanding that the WDA and UIA entered into pertaining to the provision of Wage Record data. The director must sign the form and return to the WDA no later than April 16, 2014.

The practical availability of Wage Record data through the One-Stop Management Information System (OSMIS) will be announced at a later date through a separate publication.

Action: Submit the completed Confidentiality Agreement to:

Gary Clark, Director,
Office of Talent Development Services
Workforce Development Agency
201 N. Washington Square, 5th Floor
Lansing, Michigan 48913

Inquiries: Questions regarding this policy issuance should be directed electronically to Gary Clark at clarkg1@michigan.gov.

The information contained in this policy issuance will be made available in alternative format (large type, audio tape, etc.) upon request to this office.

Expiration

Date: Continuing

GC:GC:pv
Attachment

Confidentiality Agreement for Information Received from the Unemployment Insurance Agency

Name of MW!A Director: _____

I AGREE ON BEHALF OF THE STAFF OF THE _____ MICHIGAN WORKS! AGENCY (state location/area) or DHS Work Unit (state organizational work unit):

(Please read and check-mark all boxes to indicate item has been understood and agreed to. Failure to do so will cause the Memorandum of Understanding to be rejected as to this individual.)

[] The confidential employee and/or employer information supplied by the Unemployment Insurance Agency (UIA) will be used only for the purpose stated in the Memorandum of Understanding with the Workforce Development Agency and the Department of Human Services, pertaining to the facilitation of reemployment, in accordance with Section 421.11 of the Michigan Employment Security Act and its implementing rules, and in accordance with the terms of the Memorandum of Understanding.

[] Confidential information provided by UIA for the purpose of this project will not be disclosed nor transmitted to any individuals, agencies, public or private entities, or organizations other than those approved in the Memorandum of Understanding for the purpose stated in the Memorandum of Understanding. Confidential information will remain confidential and safeguarded. No copies, duplicates or distribution to unauthorized entities or personnel will be made. Confidential information will be handled and stored in a secure environment. State and federal laws, regulations, and standards designed to protect confidentiality will be adhered to.

[] I have reviewed the attachment of 20 CFR 603.9, below, and understand its confidentiality provisions. I have been informed of the restrictions as to the legitimate use of the confidential information. I have also been informed that improper procurement, use, release or re-release of UIA confidential claimant or employer information will subject me to civil and criminal penalty provisions provided in Section 421.54(d) of the Michigan Employment Security Act, a copy of which I have been provided and have reviewed.

[] I have been informed of, and will use, the involved confidential information with acceptable security, storage, and disposal practices as outlined in the Memorandum of Understanding.

[] I will assure that my actions or inactions do not violate any of my responsibilities to protect the confidentiality of the confidential information provided by UIA.

[] I agree to immediately report to UIA any breach, improper disclosure, or impropriety regarding the use of the confidential information supplied by UIA.

[] I further agree to instruct all project personnel working at the above-identified MW!A office who may have access to confidential UIA data of all of the above provisions and secure their agreement to comply.

Signature of MWA Director

Dated:

MCL 421.54(d), Penalties:

“(d) If any employee or agent of the unemployment agency. . . willfully discloses confidential information obtained from any employing unit or individual in the administration of this act for any purpose inconsistent with or contrary to the purposes of this act . . . he or she is guilty of a misdemeanor punishable by imprisonment for not more than 90 days or a fine of not more than \$1,000, or both. Notwithstanding the preceding sentence, if any unemployment agency employee, agent of the unemployment agency . . . knowingly, intentionally, and for financial gain, makes an illegal disclosure of confidential information obtained under section 13(2), he or she is guilty of felony, punishable by imprisonment for not more than 1 year and 1 day.” (Emphasis added).

20 CFR 603.9. What safeguards and security requirements apply to disclosed information?

(a) In general. For disclosures of confidential UC information under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis); §603.5(e) (to a public official), except as provided in paragraph (d) of this section; §603.5(f) (to an agent or contractor of a public official); §603.6(b)(I) through (4), (6), and (7)(i) (as required by Federal UC law); and §603.22 (to a requesting agency for purposes of an IEVS), a State or State UC agency must require the recipient to safeguard the information disclosed against unauthorized access or redisclosure) as provided in paragraphs (b) and (c) of this section, and must subject the recipient to penalties provided by the State law for unauthorized disclosure of confidential UC information.

(b) Safeguards to be required of recipients.

(1) The State or State UC agency must:

- (i) Require the recipient to use the disclosed information only for purposes authorized by law and consistent with an agreement that meets the requirements of §603.10;
 - (ii) Require the recipient to store the disclosed information in a place physically secure from access by unauthorized persons;
 - (iii) Require the recipient to store and process disclosed information maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain the information by any means;
 - (iv) Require the recipient to undertake precautions to ensure that only authorized personnel are given access to disclosed information stored in computer systems;
 - (v) Require each recipient agency or entity to:
 - Instruct all personnel having access to the disclosed information about confidentiality requirements, the requirements of this subpart B, and the sanctions specified in the State law for unauthorized disclosure of information, and
 - Sign an acknowledgment that all personnel having access to the disclosed information have been instructed in accordance with paragraph (b)(1)(v)(A) of this section and will adhere to the State's or State UC agency's confidentiality requirements and procedures which are consistent with this subpart B and the agreement required by §603.10, and agreeing to report any infraction of these rules to the State UC agency fully and promptly,
 - (vi) Require the recipient to dispose of information disclosed or obtained, and any copies thereof made by the recipient agency, entity, or contractor, after the purpose for which the information is disclosed is served, except for disclosed information possessed by any court. Disposal means return of the information to the disclosing State or State UC agency or destruction of the information, as directed by the State or State UC agency. Disposal includes deletion of personal identifiers by the State or State UC agency in lieu of destruction. In any case, the information disclosed must not be retained with personal identifiers for longer than such period of time as the State or State UC agency deems appropriate on a case-by-case basis; and
 - (vii) Maintain a system sufficient to allow an audit of compliance with the requirements of this part.
- (2) In the case of disclosures made under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis), the State or State UC agency must also—
- (i) Periodically audit a sample of transactions accessing information disclosed under that section to assure that the entity receiving disclosed information has on file a written release authorizing each access. The audit must ensure that the information is not being used for any unauthorized purpose;
 - (ii) Ensure that all employees of entities receiving access to information disclosed under §603.5(d)(2) are subject to the same confidentiality requirements, and State criminal penalties for violation of those requirements, as are employees of the State UC agency.