

Disclosure of Information-Breach of Security

Background

The Unemployment Insurance (UI) Division collects and maintains records of claimants' personal and private information in order to administer the UI program. Employees' access to personal and private information collected in UI records is limited to the information necessary to perform their job duties. The disclosure of such information is governed by the provisions of Article 18, Section 537 of the State Labor Law. The Information Security Breach and Notification Act governs the identification and notification of key individuals of an unauthorized disclosure of an individual's or individuals' personal and private information.

Section 537 of Labor Law prohibits the disclosure of any Unemployment Insurance information acquired by employees of the Department of Labor regarding an employer or its employees to any other person or entity without a consent document on file. It prohibits the information from being open to the public or from being used in any court action with few exceptions, or from being shared with other Department divisions.

The Information Security Breach and Notification Act provides for the notification of individuals who had their personal and private information compromised. It guarantees these individuals the right to know, in a timely manner, what information was exposed in order to take necessary steps to prevent identity theft and/or repair any damage that may result. Although the Information Security Breach and Notification Act governs the breach of data from an electronic system, it is the policy of the UI Division to follow the same procedure if data on paper documents is compromised.

Consistent with the Department's policy regarding the confidentiality of individuals' personal and private information, the UI Division is committed to protecting such information in UI claim records. Division employees provided with access to personal and private information are responsible for protecting the privacy of information maintained in UI records and for the immediate notification to management if the security of personal and private information is compromised.

Definitions

Breach of Security under the Information Security Breach and Notification Act is defined as the unauthorized acquisition of data which compromises the security, confidentiality or integrity of personal and private information. A good faith acquisition of personal and private information by an employee or an agent of a state entity for the purposes of the agency is not considered a breach of the security under this law, provided that the private information is not used or subject to unauthorized disclosure.

"Personal Information" is information concerning a person which, because of name, number, personal mark, or other identifier, can be used to identify the person.

"Private Information" is personal information consisting of any information in combination with one or more of the following data elements with the exception of encrypted data without an encryption key:

- 1) Social Security number
- 2) Driver's License Number or Non-Driver's Identification Number or

- 3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Private Information" does not include information which is lawfully available to the public.

Purpose

The purpose of this procedure is to reinforce the need for UI Division employees to protect the confidentiality of UI file(s) information; and to establish a procedure for immediate notification of appropriate Division personnel when it is discovered that an individual's or individuals' personal and private information has been compromised or potentially compromised in order to initiate the notification of affected parties as required under the Information Security Breach and Notification Act.

Procedure

There are three components of this procedure required by the UI Division.

1. Identification of Breach of Security

A breach of security is an event that potentially threatens the confidentiality of an individual's personal and private information as defined in the Background section of this procedure. These events could include but are not limited to the circumstances such as:

- a) Computers, laptops, CDs, or disks containing a claimant's private and personal information are missing;
- b) An individual's personal and private information is revealed to a third party without a valid consent to do so on file;
- c) A claimant(s) receives a copy of another claimant's UI mail that lists the claimant's name, address, social security number;
- d) A claimant receives another claimant's debit card statement;
- e) An audit report listing a claimant's name and social security number is inadvertently mailed to the wrong employer;
- f) A claimant's personal and private information is inadvertently revealed to a spouse or ex-spouse without consent to do so on file;
- g) Department records containing personal and private information of an individual(s) has been downloaded or copied;
- h) An electronic device has been infected or potentially infected with a virus or worm.

2. Reporting Incidents of Breach of Security

When a breach of security of a claimant's personal and private information as defined in the Information Security Breach and Notification Act has been identified by a UI Division employee, the office director, manager or designee should be notified immediately so they can take appropriate action.

The office director, manager or designee will immediately report the breach by calling:

- a) the UI Division at 518 457-8312 and
- b) complete the UI Division's confidential [Breach of Security Incident Report form](#) and e-mail it to the: UI Division IRR at: labor.sm.uid.irr.

- c) The IRR will immediately notify the appropriate Department officials (if appropriate):
 - o Information Security Officer
 - o The Chief Information Officer.

Note: The Breach of Security Incident or the information on the Report should not be discussed outside of the normal supervisory channels in order to minimize the opportunity for identity theft.

3. Maintenance of Records

Records of Breach of Security files should be maintained for ten years.