Montana Department of
LABOR & INDUSTRY
Office of Information Technology

Advisory

November 27, 2013

To: Department of Labor and Industry (DLI) staff, contractors, and 3rd parties
Subject: Procedure for protecting personal identifiable information

---

Operational Procedures for Personally Identifiable Information

Personally Identifiable Information (PII) must be protected to ensure our customers are not unduly put at risk for identity theft. The following procedures are to be followed in regard to handling PII. These procedures will cover most situations. However, situations may arise that may require further consideration. Please bring these matters to the attention of your manager. Please remember that it is VERY important that we provide consistency with services and compliance to these directives across the state. It creates a substantial issue with our customers when different offices handle defined protocols in different ways. The success of these procedures hinges on every office implementing them consistently every time. Employees are responsible for the sensitive PII in their possession.

U.S. Mail (USPS)—the US Mail is considered a safe process for transmission of all documents.

- US Mail **can** be utilized for sending information that contains all levels of PII.
- Mail processes should be scrutinized in each office to ensure that both incoming and outgoing mail is not placed in areas that are accessible to the public. Security of the mail should be an intentional, pre-determined process, until it is in possession of the USPS.
- Envelopes utilized for mailing should be checked to ensure the contents cannot be seen or deciphered through the envelope. This may be accomplished by using security lined envelopes, using an additional sheet of paper to obscure the document being sent, or placing the first envelope inside an additional envelope.
- Make every reasonable effort to ensure that the mailing address is current.
- Do not mail postcards that contain PII.

E-Mail

- E-Mail should never be used to transmit Sensitive PII. This **may** include applications and resumes depending on their level of PII content.
    - Sensitive PII includes: SSN, Medical information, Driver's license number, Full DOB.
- Use E-pass instead of email to transmit documents that contain sensitive PII.
- If E-pass is not an acceptable method of transmission, consider fax or US Mail (following defined protocols) with consideration of required time frames and the information that is needed.
- If you need to use numbers to provide identification for information in an email, use only client ID numbers or the last four numbers of a SSN.
- In the event information containing PII is received unsolicited via email, process as necessary and delete the email. Do not forward!
- For additional guidance concerning electronic transmission of date, please refer to the IT Policy: Acceptable Use Policy.

Computer Monitors

Employees working on sensitive PII should have monitors positioned to reduce the risk of shoulder surfing

Phone & Voice

- Be aware of your surroundings! Do not hold conversations in a populated area when the discussion involves PII. When requesting a customer's identity do not request the full SSN only the last four of the Social Security number and the first three letters of the last name. **Per Unemployment Insurance please use the individual ID #**.
- When requesting PII such as an SSN do not repeat them out loud.

Fax—Fax is a secure form of transmission as long as the device receiving the fax is secure. In the case of faxing sensitive PII, you will need to verify that with the recipient. Please follow these security measures:

- To ensure that the receiving fax is secure:
  - Fax is located in an area where the public does not have access.
  - Could be located in a private office
  - Secure faxing may be achieved by calling the recipient and ensuring they are waiting to receive the incoming fax.
- Verify the fax number of the intended recipient.
  - It is crucial that the fax numbered is entered accurately.
- If you are unable to confirm the security of the receiving machine, you may use one of these options:
  - Send by US Mail
  - Scan to a secure location and send by Epass
  - Delete the sensitive PII prior to faxing. To do this, make a copy of the document. Using a marker, black out the sensitive PII and then fax. Return the original to the customer, unmarked. Shred the copy after faxing.
- If a fax is received unsolicited which contains PII, process as if it were handed to you and take every measure to secure the information as appropriate.
- Be sure that any fax machine that receives incoming documents is located in a secure area.
- For public use machines, please post a notice that states: For security of your personal information, you should confirm with the receiving party that your fax will be secure upon arrival.

Scanning

- Any documents that contain sensitive PII and need to be scanned should be scanned and saved to a secure location, such as a personal drive (P drive, H drive, etc.). Documents can be sent by ePass from that location and then deleted when no longer needed.

Clean Desk

- Be aware of the documents that are viewable on your desk or your computer screen. Take steps to ensure that sensitive PII is not viewable to others.
- Lock up sensitive PII when not present at your desk and at the end of the work day.

File Cabinets

- Must be secured at all times if it contains sensitive PII.
- Do not store sensitive PII in cabinets without locking mechanisms.

Other

- Sensitive PII must not leave the building unless authorized by immediate supervisor. The supervisor will track, monitor, and verify that the information was returned.
- Report any abuse to sensitive PII to your immediate supervisor and Information Security Manager.
- Take time at the end of each day to secure sensitive PII.