

Commonwealth of Massachusetts
Executive Office of Health and Human Services Privacy Office

DATA PROTECTION POLICY AND PROCEDURES

Effective April 14, 2003

Last revised August 14, 2015

BACKGROUND AND PURPOSE

The Executive Office of Health and Human Services (“EOHHS”) is the principal executive office in the Commonwealth for developing, coordinating, and administering health and human services within the Commonwealth and, among other things, is authorized to act as the single state agency responsible for administering the Commonwealth’s Medicaid Program and its Children’s Health Insurance Program (together known as MassHealth). In performing its responsibilities, EOHHS regularly acquires or otherwise comes into contact with protected health information (“PHI”) and other types of personally identifiable information (“PII”) regarding MassHealth applicants and beneficiaries and other individuals.

The EOHHS Chief Privacy Officer (“Privacy Officer”), as overseen by the EOHHS General Counsel, is responsible for overseeing the privacy program for the following EOHHS offices: the Office of the Secretary, the Office of Medicaid (also known as MassHealth), the Health Safety Net Office, and the other offices within EOHHS performing activities for EOHHS and its constituent agencies at a consolidated level (e.g., the Office of Financial Management, the Office of Administration Services (which includes, without limitation, EOHHS IT), the Office of Human Resources and the Office of Leasing and State Owned Property (also known as Facilities)).¹ Such privacy program is implemented by the Privacy Officer and other members of the EOHHS Privacy Office staff, acting under the supervision of the Privacy Officer.

The EOHHS Privacy Office (“Privacy Office” or “PO”) is committed to preserving the privacy and security of all PHI and other PII that EOHHS obtains, creates or otherwise deals with in the course of its business in compliance with its obligations under state and federal laws and regulations, including M.G.L. c. 93H, 93I and 201 CMR 17.00, the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), and the Privacy, Security and Breach Notification Rules implemented thereunder at 45 CFR Parts 160 and 164 (“HIPAA Rules”), other applicable federal and state laws and regulations,² and applicable contracts to which EOHHS is a party.³ This policy and its related procedures are intended to ensure that EOHHS’ workforce maintains the privacy and security of PII in accordance with such legal obligations.

¹ For purposes of this policy and related procedures, “EOHHS” should be read to refer only to these discrete offices within EOHHS. For the avoidance of doubt, it should not be read to include any EOHHS constituent agency.

² Additional privacy and security laws and regulations include, without limitation: (a) Section 1902(a)(7) of the Social Security Act (42 USC §1396a(a)(7)) and the federal Medicaid regulations implemented thereunder (42 CFR Part 431, Subpart F); (b) federal regulations governing the privacy of substance abuse records (42 CFR Part 2); (c) federal privacy and security regulations implemented pursuant to the Affordable Care (45 CFR §155.260); (d) the Massachusetts Fair Information Practices Act (M.G.L. c. 66A); and (e) and the Massachusetts breach reporting statute (M.G.L. c. 93H) and data destruction (M.G.L. c. 93I).

³ Applicable contracts containing privacy and/or security restrictions include, without limitation, Interagency Service Agreements between EOHHS and the Massachusetts Department of Revenue, a Computer Matching Agreement between EOHHS and the Centers for Medicaid and Medicare Services, and the Computer Matching Agreement between EOHHS and the Social Security Agency.

For the purposes of this policy and related procedures, “EOHHS” refers to the EOHHS Secretariat, which consists of the Office of the Secretary, MassHealth (also referred to as the Office of Medicaid), the Health Safety Net Office, and the other offices within the Secretariat performing activities for the EOHHS Secretariat and EOHHS constituent agencies at a consolidated level (the Office of Financial Management, the Office of Administration Services (which includes, without limitation, EOHHS IT), the Office of Human Resources and the Office of Leasing and State Owned Property (also known as Facilities)).

APPLICABILITY

This policy and its related procedures apply to all PII, including PHI. PII is any information that identifies a specific person, or could potentially be used, either alone or combined with other information, to identify a specific person.⁴ For example, the following information may be considered PII: name, such as full name, maiden name, mother’s maiden name, or alias; (b) personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number; (c) address information, such as street address or email address; (d) asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people; (e) telephone numbers, including mobile, business, and personal numbers; (f) personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry); (g) information identifying personally owned property, such as vehicle registration number or title number and related information; and (h) information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).⁵ Aggregate data may also be considered PII unless it has been properly de-identified.⁶

PII includes (but is not limited to) PHI. PHI is a subset of PII that relates to the physical or mental health of the individual, the provision of health care to the individual, or the payment for health care for the individual.⁷ PHI is subject to privacy and security restrictions under HIPAA and the HIPAA Rules. Additionally, a number of other federal and state laws and regulations applicable to EOHHS regulate the privacy and security of PII.⁸ PII also may be subject to privacy and security restrictions under contracts between EOHHS and one or more third parties.⁹

All members of EOHHS’ workforce must follow this policy and related procedures. For purposes of this policy and procedures, “EOHHS’ workforce” includes all EOHHS employees as well as all independent contractors, consultants, interns, and volunteers who perform services for EOHHS and under EOHHS’ control. This policy and related procedures also apply to all other persons who are authorized to access PII, including consultants, contractor employees and agency and other government personnel who are

⁴ Information contained in or that otherwise constitutes a public record (as defined in, and subject to the exceptions set forth in, M.G.L. c. 4, §7(26)) for purposes of the Massachusetts Public Records Law (M.G.L. c. 66, §10) is not considered PII for purposes of this policy and related procedures.

⁵ See National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Special Publication 800-122.

⁶ See 45 CFR 164.514 and/or contact the Privacy Office for guidance on de-identification.

⁷ See 45 CFR 160.103 for the complete definition of PHI.

⁸ See footnote 2 for a non-exhaustive list of other privacy laws and regulations applicable to various types of PII.

⁹ See footnote 3 for a non-exhaustive list of contracts with impose additional privacy and/or security restrictions on various types of PII.

provided with or granted access to PII for a purpose permitted by law. For the purposes of this policy and related procedures, all such other persons are referred to as “third-party workforce.”

All members of EOHHS’ workforce and third-party workforce members to whom this policy and related procedures apply are required to review this policy and procedures and to affirm their acknowledgement of, and agree to adhere to, such policy and procedures. EOHHS Human Resources and/or the Privacy Officer will retain this affirmation.

STATEMENT OF POLICY

As a member of EOHHS’ or a third-party’s workforce, you must treat all PII with the highest regard for the individual’s confidentiality and privacy. You may only use, share, and request PII as permitted by applicable law and contract and as necessary to perform your job. When using such information, you must make reasonable efforts to access and use the minimum amount of PII necessary to perform the intended function. When sharing PII with, or requesting PII from, other entities or persons, including other workforce members, you must make reasonable efforts to share or request the minimum amount necessary to perform the particular activity for which the PII was shared or requested. If sharing PII with other entities or persons, including other workforce members, you must ensure that such entity or person is authorized to access such PII.

Generally, you must:

- Not access PII unless necessary to perform your job;
- Not attempt to access PII you are not authorized to access;
- Not attempt to circumvent any EOHHS systems security mechanism;
- Not share PII with other members of EOHHS’ or third-party workforce, unless necessary to perform your job;
- Not share PII with other members of EOHHS’ or third-party workforce, unless you know they are authorized to access PII;
- Not discuss PII in public areas, such as in lobbies, hallways, and elevators;
- Not disclose or discuss PII after you leave EOHHS premises or employment; and
- Immediately report known or suspected privacy and security incidents in accordance with the procedures contained herein.

You must also comply with the specific privacy and security procedures set forth in this document and any additional policies, procedures and/or protocols that may apply based on your job function, your employer, or other factors.

Additionally, if you have access to PII that is subject to “heightened” privacy or security restrictions under applicable law, regulation or contract, you must also comply with all such restrictions. PII that is subject to heightened privacy and/or security restrictions includes:

- Information that EOHHS receives from certain providers and managed care entities regarding a person who received a diagnosis related to drug or alcohol abuse, treatment for drug or alcohol abuse or a referral for such treatment.
- Information that EOHHS receives from the following state and federal agencies:
 - Massachusetts Department of Revenue
 - Massachusetts Registry of Motor Vehicles
 - Social Security Administration
 - Internal Revenue Services
 - Department of Homeland Security
 - Centers for Medicaid and Medicare Services

- Any other information that EOHHS receives from a third party and that is subject to privacy and/or security restrictions under a contract to which EOHHS is a party.

If you have any questions about what information is subject to heightened privacy and/or security restrictions or how to comply with such restrictions, contact your supervisor and/or the Privacy Office.

PROCEDURES

I. WORK-SITE PRACTICES

You must:

- Not leave your computer or terminal unattended without first locking your computer. You must log off or activate password protection before leaving computers or terminals unattended.
- Store paper containing PII in locked rooms and filing cabinets whenever possible.
- Remove paper containing PII from printers, fax machines, scanners, and other common areas, such as conference rooms and meeting rooms, as soon as possible.
- Not leave PII in plain view of unauthorized persons in any area including on office devices such as computer screens or portable electronic devices such as smartphones or laptops. Position your workstation so that the monitor is not visible to the public when working near public areas.
- Log off or shut down your personal computers when leaving the office for the day.
- Not print out PII, or remove PII in any form from EOHHS premises, unless necessary to perform your job, within the scope of your authorization, and as approved by your supervisor. You must return the PII to EOHHS premises as soon as the off-premises function is completed.

II. NETWORK PASSWORD PROCEDURES

You must not share your passwords or user IDs with anyone else, store written passwords anywhere near your workstation, access EOHHS systems under someone else's user ID, or allow anyone else to access EOHHS systems under your user ID. In addition, EOHHS IT requires the following password protections:¹⁰

- Personal laptops should not be connected to the EOHHS Network before they have been checked for viruses by EOHHS IT Staff and approved to be attached to the EOHHS Network by the EOHHS Security Office.
- Smartphones used to access PII must be formally approved pursuant to the requirements of the EOHHS Mobile Device Policy.
- Authorized users are responsible for all activity performed under his/her User Login ID and password
- All EOHHS and third-party workforce members must prevent unauthorized users from gaining access to or using his/her User Login ID or password.
- EOHHS follows standard Commonwealth password methodology. In general, passwords:
 - ✓ Must be unique
 - ✓ Must be minimum of eight characters in length
 - ✓ Must be changed every 60 days
 - ✓ Cannot be repeated for 25 iterations
 - ✓ Must not be a proper name or similar word, which may be guessed
 - ✓ Should consist of three of the following: (1) upper case letter; (2) lower case letter; (3) number; and (4) symbol.

¹⁰ See Information Security (Executive Order 504) –Employee Learning Guide p. 10

- **Please Note:** Password requirements vary from system to system; contact your system administrator for assistance if necessary.
- **If Your Password Is Compromised:** Change your password immediately and report the situation to the EOHHS IT Helpdesk or Chief Security Officer (“CSO”). This includes when your password is stolen or accidentally shared. EOHHS Security Office or IT Help Desk staff will work with you to ensure that your ID, computer, and files are secure.

You must report all violations of this policy and procedures to the CPO and CSO.

III. PROTECTING AGAINST THEFT

A common information security issue involves the theft or loss of computer equipment. Computers, particularly laptops, as well as floppy discs, USB Flash Drives, CDs, and handheld electronic devices can easily be stolen if left unattended. Always be sure to keep your computer equipment secure at all times, especially when traveling. PII stored or accessed on a portable device must be encrypted. Encrypted flash drives may be available from your program coordinator or EOHHS IT upon request. In general, EOHHS and third-party workforce members may not remove PII from the workplace without authorization from their supervisor and/or the EOHHS Privacy Officer or CSO.

IV. SECURITY THREATS INTRODUCED FROM THE INTERNET; SECURITY INCIDENTS

Potential threats related to Internet use include viruses, trojans and worms that are designed to destroy your computer system, disclose information, damage your files and disable your software. Security threats can come from infected email messages, or Internet downloads. **Do not open files, email attachments, or links unless you know the origin of the file or link and/or know the person who sent it to you.** These threats are difficult to detect, easily spread and difficult to remove.

Protecting Your Computer From Viruses, Trojans And Worms

- Never open any email attachments or links sent to you from an email address you do not recognize
- Do not download files from websites that you do not know
- Inform your the EOHHS CSO or IT help desk if you think your PC is infected
- Never attempt to fix a virus by yourself

Other Safeguards

Beware of non-authorized people seeking information such as:

- Phishing (illegitimate email requests for information)
- Impersonation (as agency IT staff via email, over the phone)
- Shoulder surfing (someone looking over your shoulder while you use your computer)

V. TRANSMITTING PII

Before faxing, emailing, mailing, or otherwise transmitting PII, you must be certain that the disclosure of PII to the intended receiver is a permitted and authorized disclosure. If you are uncertain about the appropriateness of the disclosure, please consult with your supervisor or the EOHHS Privacy Office.

Secure Email Procedures

Emails containing PII may be sent from any address that ends in “**state.ma.us**” to any other address that

ends in “state.ma.us.” However, EOHHS workforce **must** use EOHHS’ **Secure Email Procedure** when sending, replying to, or forwarding it to any other email address.

1. Type “**Secure:**” at the beginning of the SUBJECT line of the e-mail, unless you are replying to or forwarding an e-mail that already has “**Secure:**” at the beginning of the subject line. The system will look for that prefix and automatically encrypt and secure the e-mail, including any attachments.
2. If “**Secure:**” does not appear at the beginning of the subject line, the e-mail will **NOT** be secure.
3. Third-party workforce should consult with their employer’s privacy or security office or other appropriate individual for guidance on how to email PII securely.

Facsimile Procedures (Fax)

1. Call to let the receiver know you will be sending a fax containing PII and to confirm the fax number. Ask the receiver to attend the fax machine until transmittal is complete, unless the receiving fax machine is in a locked, limited-access location, or the receiver uses a desktop application. Ask the receiver to let you know when the fax is received.
2. Use a fax cover sheet that contains MassHealth’s standard confidentiality statement (or a similar confidentiality statement, in the case of third-party workforce). Complete all fields including names of sender and receiver, and number of pages.
3. Use pre-programmed fax numbers when possible.
4. Make sure the fax confirmation option is activated. Verify transmission with fax activity confirmation sheet.
5. If transmission is successfully completed, remove the documents from the vicinity of the fax machine, including fax activity confirmation sheets. Keep fax activity confirmation sheets with original documents. If transmission cannot be completed, call and let receiver know there has been a problem, and remove the documents from the vicinity of the fax machine.
6. If receiver does not confirm receipt within a reasonable period of time, call to determine if fax has been received.

Electronic Data Interchange (EDI), Secure File Transfer Protocol (SFTP), or other Third-Party Secure Document Service

1. Secure third-party document delivery services, EDI, and SFTPs may be used to transmit data, including PII.
2. EOHHS workforce should consult Systems Support Desk personnel for further instruction on using these methods to transmit PII.
3. Third-party workforce should consult with their employer’s privacy or security office or other appropriate person for further instruction.

Physical Means other than U.S. mail (e.g., by hand, courier, or expedited delivery service such as FedEx or UPS)

1. PII (in any form, including hard copy or electronic media) may be transmitted by physical means.
2. Double-check the contents of the mailing to ensure that only the correct PII is included.
3. Ensure that the envelope is well-sealed and unlikely to come open during routine mail handling.
4. Mark package “Confidential.”
5. Verify the identity of the individual picking up the package.
6. Retain tracking number, if applicable.
7. If the receiver informs you that information was not received, contact delivery service to track item, if applicable.

U.S. Mail (USPS) (other than system-generated mailings)

1. When sending PII via USPS, mark the envelope “Confidential.”
2. Include your name along with the return address.
3. Double-check the contents of the mailing to ensure that only the correct PII is included.
4. Ensure that the envelope is well-sealed and unlikely to come open during routine mail handling.

VI. REMOVING PII FROM EOHHS PREMISES

EOHHS and third-party workforce members may not remove PII in any form from the workplace without authorization from their supervisor and/or the Privacy Officer or EOHHS CSO. If you need to store or access PII on a portable device for authorized business purposes, it must be encrypted. Encrypted flash drives may be available from your department coordinator or EOHHS IT upon request.

Removing computer hardware containing PII from EOHHS premises

1. When computer hardware is signed out, contact the Systems Support Desk to follow the proper computer hardware sign-out procedure.
2. When computer hardware is removed permanently from EOHHS premises, make sure the Systems Support Desk reformats the hard drives so that all data is removed.

VII. RETENTION/DISPOSAL PROCEDURES

All EOHHS and third-party workforce members are required to maintain PII in accordance with the appropriate schedules.¹¹ **When disposing of PII**, you must first consult the applicable retention schedule and any applicable department or agency-specific protocols to confirm that that data/information is appropriate for disposal. In all cases, PII must be properly disposed in accordance with state and federal law and regulations. If you have any questions, please consult your supervisor.

Paper: If the PII may be disposed of according to retention procedures and agency protocols and is in paper form, dispose of it by one of the following two methods:

1. Shred the documents; or
2. Place documents in a locked recycle bin.

Other Media: If the PII may be disposed of according to retention procedures and agency protocols and is on audio tape, video tape, compact disc (CD), digital video disk (DVD), thumb drive, or any other type of electronic/magnetic hard media, EOHHS workforce should contact Facilities Management for proper destruction of the material. Third-party workforce should consult with their employer’s security office or other appropriate individual for instruction as to proper disposal.

VIII. THIRD PARTY REQUESTS FOR PII; IDENTITY VERIFICATION PROCEDURES¹²

Before disclosing any PII to an outside party, you must be certain that the disclosure is a permitted and authorized disclosure. If the disclosure is not permitted and authorized, do not disclose any PII (including whether an individual is a MassHealth member). If uncertain about the appropriateness of the disclosure, consult with your supervisor or the Privacy Office. Additionally, consult with your supervisor or the Privacy Office before responding to any request for PII from an outside party that does not fall within the scope of your normal job function.

¹¹ See Massachusetts Statewide Record Retention Schedule for minimum retention periods. In some instances, other retention schedules requiring longer retention periods apply, e.g. Federal Records Retention Schedule (44 USC 3303a), etc.

¹² All references to MassHealth members in these verification procedures should be read to include MassHealth, Health Safety Net and Connector program applicants and beneficiaries.

If the disclosure is permitted and authorized, follow the identity verification procedures set forth below.

Verifying Identity of Members

1. **By telephone:** MassHealth members must give their social security number or MassHealth ID number and date of birth, which must be checked against MassHealth records.
2. **In person:** MassHealth members must present their MassHealth card together with another form of identification. If a member cannot provide his or her MassHealth card at the time of contact (or does not have a MassHealth card), you may verify the member's identity by requesting that the member provide his or her social security number or MassHealth ID number and date of birth, which must be checked against MassHealth records. Another form of identification must also be provided.

Verifying Identity of Personal Representatives

1. **By telephone:** The personal representative of a MassHealth member (which includes an authorized representative, appeal representative, and all others who have legal authority to act on behalf of the member, such as a parent or legal guardian) must be listed as such on MassHealth's records. The personal representative must also give the member's MassHealth ID number and date of birth. The representative status and member information must be checked against MassHealth records.
2. **In person:** The personal representative must provide the above information as well as another form of identification.

Verifying Identity of a Provider

1. **By telephone:** A provider calling must give his or her MassHealth Provider Number, which must be checked against MassHealth records.
2. **In person:** A provider must give his or her MassHealth Provider Number, which must be checked against MassHealth records, and provide another form of identification.

Verifying Identity of Others

1. **Persons to whom a disclosure is permitted without member authorization**
 - a. **By telephone:** Other persons to whom a disclosure is permitted without the member's authorization must verify their identity by stating their name, place of employment, purpose of the disclosure, and other identifying information specific to their inquiry, such as a claim number.
 - b. **In person:** The above information must be provided as well as another form of identification.

If the nature and content of the inquiry do not sufficiently confirm identity, or raise questions about the appropriateness of the disclosure, you should consult your supervisor before making the disclosure.

Other Identity Verification Procedures

1. If you routinely deal with a caller and you recognize the caller's voice, you may confirm his or her identity orally.
2. If a requestor cannot verify his or her identity as described above, do not disclose any member information. Contact your supervisor or the Privacy Office.
3. Depending on your role, your supervisor may provide additional or supplemental verification procedures or protocols that apply to situations not covered by this document. If any such contemplated additional procedures or protocols conflict with the procedures set forth in this document, the procedures in this document shall apply absent approval of an exception to these procedures from the Privacy Office.

If any questions regarding a person's identity remain after following the above verification procedures, do not disclose any PII to such person and consult with your supervisor and/or the Privacy Office.

IX. REPORTING PRIVACY AND SECURITY INCIDENTS

You must immediately report any incident involving the known or suspected **privacy incident** to the Privacy Office at privacy.officer@state.ma.us. A privacy incident is the acquisition of PII by an unauthorized person or entity, the disclosure of PII to an unauthorized person or entity, or the access to or use of PII by an unauthorized person or entity or for an unauthorized purpose. Examples of privacy incidents include:

- A violation of these procedures
- Faxing documents that contain information about a MassHealth or Health Connector plan applicant or member to the wrong fax number
- The loss or theft of a computer, computer disc, USB Flash Drive, or smart phone that contains or may contain PII
- The loss or theft of paper records that contain PII
- Confirming to a third party that a person is a MassHealth applicant or member without verifying that the third party is authorized to receive such information
- Leaving papers or other materials containing PII in public areas
- Mailing PII to an incorrect address
- Evidence of unauthorized or inappropriate access, viewing, copying, or removal of PII
- Disclosing PII about a member or other individual without verifying the requestor's authorization and identify
- Viewing the PII of friends, neighbors or public personalities (including, for example, checking MassHealth records to see if your neighbor is a MassHealth beneficiary)
- Sending an unsecured email containing PHI or PII

You must immediately report known or suspected **security incidents** to the Systems Support Desk at systemssupporthelpdesk@massmail.state.ma.us or 617-367-5500. A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII or interference with system operations in an information system containing PII. Examples of security incidents include:

- A disruption of computer services caused by a virus, trojan, or a worm
- The loss of a computer, computer disc, USB Flash Drive, or Blackberry that contains or may contain PII
- The presence of an unauthorized person in a secured facility where PII is stored
- Evidence that the password or secure login credentials to a system or database containing PII has been compromised (for example, receiving notification that your password has been changed when you did not change it)

A single incident may be reportable as both a privacy incident and a security incident. If in doubt, contact your supervisor and/or report the incident to both the Privacy Office and the Systems Support Desk.

You should also notify your supervisor of any known or suspected privacy or security incident.

X. EXCEPTIONS

In some instances, the Privacy Office, with approval by EOHHS General Counsel, may permit

exceptions to this policy and related procedures.

XI. SANCTIONS

Failure to comply with the policies and procedures set forth in this document may result in suspension of access, and/or disciplinary action, up to and including termination of employment. In some cases, violations may be grounds for civil action or criminal prosecution. Sanctions for non-compliance with this policy and related procedures will be handled in accordance with applicable laws and regulations, collective bargaining agreements, civil service rules, and EOHHS procedures and/or contractual agreements relating to third-party workforce.

QUESTIONS

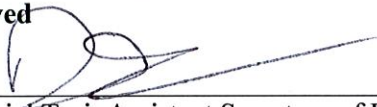
Please contact the **EOHHS Privacy Office** if you have any questions.

E-mail: privacy.officer@massmail.state.ma.us

Telephone: 617-210-5308

APPROVAL


Approved



Daniel Tsai, Assistant Secretary of EOHHS and Director
of MassHealth

8/14/15

DATE



Jesse Caplan, General Counsel of EOHHS

8/14/15

DATE

Commonwealth of Massachusetts
Executive Office of Health and Human Services Privacy Office

Privacy Training Affirmation Statement

I _____ have read the EOHHS Privacy Office Data Protection Policy & Procedures (DPP).

- I understand that this policy and these procedures apply to me and agree to adhere to them.
- I understand that this policy and related procedures are available to me via the EOHHS Intranet, and that I may contact my supervisor or the EOHHS Chief Privacy Officer with any questions.
- I understand that unauthorized use, access or disclosure of personally identifiable information is prohibited.
- I understand that if I am authorized to access personally identifiable information received from another state or federal agency or other third party, I must comply with all additional privacy and security obligations applicable to the information or to my access to systems containing the information. Information that is subject to additional obligations includes information received from the Department of Revenue, the Social Security Administration and the Internal Revenue Service, as well as information received through the Federal Data Services Hub.
- I understand that failure to comply with these policies and procedures may result in suspension of access, and/or disciplinary action up to and including termination of employment. In some cases, violations may be grounds for civil action or criminal prosecution under applicable state and federal law. Sanctions for non-compliance with DPP will be handled in accordance with applicable laws and regulations, collective bargaining agreements, civil service rules, and EOHHS procedures and/or contractual agreements relating to third-party workforce.

Print Name: _____

Signature: _____ Date: _____

Job title: _____

Employer (if other than EOHHS): _____