IDENTIFYING AND SAFEGUARDING PERSONAL INFORMATION TRAINING

Executive Office of Housing and Economic Development

December 2016

Training Certification

At the end of this training presentation you will have the opportunity to submit your name to certify you have completed this training. Thank you.



Agenda

Introduction This training is a requirement pursuant to **Executive Order 504 Identifying Personal** What, when, and where to identify Personal **Information** Information Safeguarding How to safeguard Personal Information Personal **Information EOHED** and Legal Why you are required to safeguard Personal **Underpinnings** Information Conclusion YOU are responsible for identifying and safeguarding Personal Information

Executive Order 504: Regarding Security and Confidentiality of Personal Information

Click below to see EO:

http://www.mass.gov/courts/docs/lawlib/eo500-599/eo504.pdf

"Identity theft is a serious crime..."

The EO charges the Commonwealth to adopt and implement the maximum feasible measures reasonably needed to ensure the security, confidentiality, and integrity of Personal Information.

The EO requires ALL state employees to take immediate and affirmative steps to comply with the EO.

Key Governing and Related State Laws and Regulations

MA General Law or Code of Regulations	Subject
M.G.L. c. 66	Public Records
M.G.L. c. 4, §7(26)	Exemptions to Public Records
M.G.L. c. 66A	Fair Information Practices
M.G.L. c. 93H	Security Breaches
950 CMR 32.00	Public Records Access
201 CMR 17.00	Standards for the Protection of Personal Information of Residents of the Commonwealth

Maintain and Safeguard Personal Information

- System Security
 - Consider that each network device is an entry point (computer, laptop, smartphone, server).
 - Employee computers are part of the agency's network.
- □ Comply with the EOHED's Acceptable Use Policy
 - Do not access or disseminate Personal Information unless required by your job.
 - Never share passwords.
- Comply with Specific System User Account Requirements
 - Use strong passwords.
 - Don't use somebody else's password or user ID.

EOHED Information Security Program

□Goal of Information Security Program (ISP):

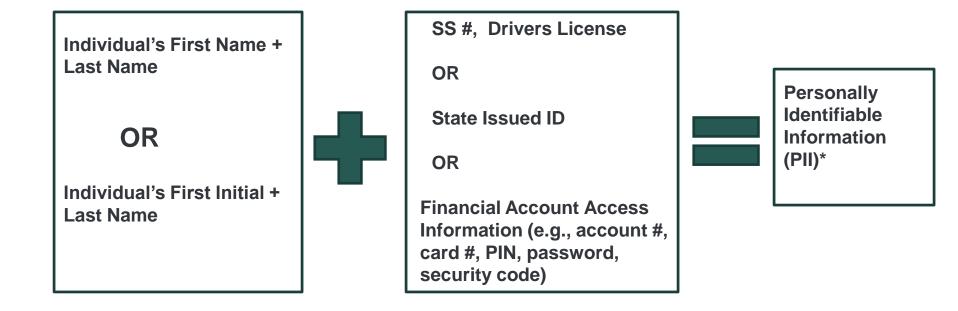
Adopt and implement the <u>maximum feasible measures</u> reasonably needed to ensure the security, confidentiality and integrity of Personal Information.

□Under EOHED's ISP, All Employees Must:

- Collect the minimum quantity of Personal Information reasonably needed to accomplish legitimate purpose for which information is being collected.
- Securely store and protect Personal Information.
- <u>Disclose Personal Information</u> and data only on a need to know basis.
- <u>Destroy</u> Personal Information and data as soon as it is no longer needed or required to be maintained under state or federal law.

Personal Information

(as defined by M.G.L. c. 93H, § 1)



*Throughout this training, we will use "PII," the universally accepted acronym for **P**ersonally **I**dentifiable **I**nformation, which means the same as Personal Information.

Personal Data

(as defined by the Fair Information Practices Act - FIPA)

Any information concerning an individual, which because of:

- 1) Name
- 2) Identifying Number
- 3) Mark
- 4) Description



Can be readily associated with a particular individual



Personal Data

Examples of PII







Molecus Cher. Zho West Hares Cherch Cher. Zho West Hares Cherch Cher. Zho West Hares Cherch C	Name				Todar's Date: //
Dept. Top Work Priories					
Concelled Of Applicables) Description Accordance of Medical Description Descript					
Bine Dame. Social foresting # Loss few Bines. No. November 1 No. November 2 No. No. November 2 No.				Zipi	
Name of Merical Denom Medical History Lar Medical Care Lar Deposition on placing to moleculary Deposition on placing to moleculary Deposition on placing to moleculary Lat are moleculary may use of posteding and community may make that Lat are moleculary may use of posteding and community may make that Lat are moleculary may be made to make the moleculary and be most or moleculary and Lat are sufficient may be made that remode synchrony could, prominent eyes, gluarems, actual disease, or presentation or existency press of the fifthering that pure have had remode synchrony could, prominent eyes, gluarems, actual disease, or presentation or existency Days were gluined Days were conscioused Days of the place of the post	Goardian (If Applicable):				
Medical History Do you have not sharpes to moderations. This is a possible processor of the	think Dusc ///	Social S	examin #		/Last Eye Esses///
Medical History Do you have not sharpes to moderations. This is a possible processor of the	Name of Moderal Discour				De Village
Medical History Despotes our of stagies to medications: List on medications put the Evoluting and community on, uptice, septice, our the counter medications and bone more despoted by the property of the pr					L-Materian I
Last all major superes, rengatios and/or hospitaleoistos you kine last Last any of the federang that you have had a record eye, here eye, deverage, critick, prominent you, glacerum, extract disease, eye principies on eye injury. Last any of the federang that you have had a record eye, here eye, elevation or eye injury. Last any of the federang that you have been a promoting or of hereoft. Last any of the federang that you have been a promoting that the hard of hereoft in your promoting that the hard of hereoft in your promoting the federang per of critical hard. Last any of more known. This part of the hard of the har		of Cha	Dju	If you	suplain
Lie ary of the Edward that you have had remoud eye, her ext. developing with promisent you, pleasants, extract disease, or go relatives on eye inform. The state of the state	List are molications you take (including	position	modeto	o, ispiris	, over the country medications and bonse remedies;
Lie ary of the Edward that you have had remoud eye, her ext. developing with promisent you, pleasants, extract disease, or go relatives on eye inform. The state of the state			-		
Lie ary of the Edward that you have had remoud eye, her ext. developing with promisent you, pleasants, extract disease, or go relatives on eye inform. The state of the state			-	-	
Lie ary of the Edward that you have had remoud eye, her ext. developing with promisent you, pleasants, extract disease, or go relatives on eye inform. The state of the state				11.45	
The resistance of the second o	List all mujor injuries, rangeries and/or	datipod	nelons yo	a have be	d
The resistance of the second o					
DISAMENE/CONDITION NO VIS	epe inflactions or eye injury: Are you programs and/or marring? Do you were glassed?	lm D	yes yes If y	on, hour o	ikl is your present pair of lensest
Blackers	epe infactions or eye injury. Are you programs and/or mannings Do you were glassed Do you were consect lenses Type of contact lenses Rapid S Family History.	In D	yes Wy yes Wy yes Wy Extended	or, how o	All to your present pair of kencel All to your present pair of kencel Other Aus they comfortable Type Tran
Content Cont	ept infactions or eye injury. Are you progrant and/or namings Do you were glassed Do you were connect lesses Type of connect lesses Ragel S Family History Hears note any family binney (puress).	Ino O Ino O Ino O Ino O	yes yes If y yes If y fixunded	or, how o	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Consultips	spe infactions or eye injury. Are you programs and/or manings Do you were glassed Do you were consect lenses Type of contact lenses Rapid S Family History Please note any family binney (puress).	Ino O Ino O Ino O Ino O	yes yes If y yes If y fixunded	or, how o	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Giorecce Mende Department Bossal Descriptors/Dissass Antiesis Canas Deleters Deleter	epe infections or sycinjery: Are you proposed and/or namings O Do you were glassed D Do you were glassed D Do you were consistenced O Type of contact, thouse O Regid O S Family History Please now are family history (pursue, DISEASE/CONDITION Blindson	In Din Din Din Din Din Din Din Din Din Di	yes liyes lify yes lify yes lify fixmoded was, slide VHS	West D	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Menshir Degenosies	eye infections or eye injery: Are you progent earl or namings Do you were glossed or Do you were contest lenses: Type of contact homes: Theyd DE Fundy History Haste rose any faculty history question Histories Histories Contact Contact	In O	yes Hy lyes Hy lyes Hy lixended	on hour or hou	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Anisotic Ani	rep infections or sylvingery. Any you progness each for encourage. Do you were glasses. Do you were connect tensor. Type of contact home. The glass of the progness of the	In O	yes If ye	or, how or	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Artheris Carar Daleten Daleten Har Dhone Hay Blacd Presure Lips Blacd Presure Lips Blacd Presure Lips Caracter	eye atlection or eye injury. An you purpose only for namenge. The your purpose of the property	Im Din	yes true if yes	or, how or	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Grane Dations Dations Hear Disease O	on adication or opinigary Any you pregnate and/or renaining Do you over glosses Do you were control thereor Type of contact himses Type of contact himses Dispass not as or fursily himsey pureau Bishares Centrar Contrar	Im Din	yes lyes Hy yes Hy Houndard	on town on town or tow	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Dates	on admission or opinitary on the Amy you prepare and/or resump? Do you were contect tensor? Type of contact house. They of the Type of contact house. They of the Type of contact house. They of the Type of Type of the Type of Typ	In District Or Co.	yes Hy Ye	War I	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Heart Discret	gu attachus or otwisters Are you puguant and/or rentrings Do you to our glosses Do you weet control thesees Thyse of contact history The output of the output of the output Desire of the output Desire outp	In Distriction Co.	yes Hy Ye	Wor I	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
High Blood Pressure	on infection on opinings. Any symposites of the manage of the company of the comp	In O	yes Ity yes Ity yes Ity yes Ity yes Ity founded VES	Wer I	All to more present pair of lemend All to your present pair of lemend J Other An they comfortable J yea J au may living or document for the Individual youthings
Kilner Diense D D D D D D D D D D D D D D D D D D D	on infection or opinings. Any symposis and on reasong of the two proposed only on the control of	In O	yes Hy yes Hy yes Hy founded VES	West of the contract of the co	All to more present pair of kensed All to pair present pair of kensed J Other An they cantiouslike J yea J au may kense of documents for the believe any socialisms:
Lapse D D D D Thrond Disease D D D D	no Markins on Opinigry And you present and the Any progress and the Any present forces. They of context hance — Displic 202 Press for one as feath belone present, and the Any present new as feath belone present for the Any	In O	yes I'ves II'vyes II'v	West of the state	All to more present pair of kensed All to pair present pair of kensed J Other An they cantiouslike J yea J au may kense of documents for the believe any socialisms:
Thyroid Disease D D D D	gen bleichen er op blegte. Aus yn progent of her on monge Do yn wer general foreit Do yn wer general foreit Do yn wer general foreit Type of counts have Type of counts Top of the count Type of the c	In Committee No	yes Ity yes Ity yes Ity yes Ity yes Ity timeded	Ser and a paramanana	All to more present pair of kensed All to pair present pair of kensed J Other An they cantiouslike J yea J au may kense or document for the believing sensitions:
	on Michael on reprint of the American of the International Company of the International Company of the International Company of International Comp	NO OCCOORD	yes Ity yes Ity yes Ity yes Ity yes Ity yes Ity founded VIIS	o have	All to more present pair of kensed All to pair present pair of kensed J Other An they cantiouslike J yea J au may kense or document for the believing sensitions:
Other O O O	gen infection or springer. And say springers and say a springer Doys were centered to Doys out a service of Doys of the Company of the Compan	NO COCCOCCOCCO	ves ves Hy ves Hy ves Hy frameded VES O O O O O O O O O O O O O	o have	All to more present pair of kensed All to pair present pair of kensed J Other An they cantiouslike J yea J au may kense or document for the believing sensitions:

What PII is NOT:

✓ Information contained in a public record (MGL c. 4, § 7(26),

✓ Intelligence information, evaluative information,

OR

✓ Criminal record information (as defined in MGL c. 6, § 167), which shall be governed by the Criminal Offender Record Information Act (CORI).

Where PII May "Live"



- Letters
- Faxes
- Printouts
- Memos
- Sticky Notes
- Trash



- File Cabinets
- Desks
- Printers or Faxes
- Laptops
- On One's Person
- Servers



- PDAs
- Cellphones
- Email
- Flashdrives
- Voicemail
- Back-up Tapes

Physically Protect PII

- Security desk/reception desk: Visitors must sign in.
- Access ID: Everyone must have access pass to enter offices.
- Lock file cabinets.
- Do not leave PII unattended in non-secure environment.
- Network devices need to be secure and only used by authorized staff.
- Use (encrypted) Secure File Email Delivery (SFED) if you must send documents with PII.
- Password protect files if they contain PII.
- Log off or lock desktop when you step away from your computer for an extended period of time during your workday.

Verbal propagation of PII needs safeguarding:
Only discuss PII when appropriate and only discuss in private spaces.

Safeguarding PII

Collect Minimum
Quantity

Disclose PII only on a NEED-TO-KNOW basis Complete Data Exchange Acknowledgement

Protect Your Passwords

- If you don't need it, don't ask for it.
- Only access info necessary for the proper performance of your job.
- De-identify data at time of collection, input, querying as much as possible.
- If you receive a request for PII outside of the normal course of program management, escalate the request before responding.
- Beware of nonauthorized people (e.g., social science researchers) seeking info (or means to access PII).

- Complete it if data is sent outside.
- Contact EOHED Information Security Officer for a copy of the acknowledgement.
- Never share your passwords.
- Make computer and file passwords unique.
- Place a "Do Not Forward" disclaimer on outgoing documents with PII in them.

EOHED is a large "network" of staff and providers:

- Approximately 900 employees
- Hundreds of business partners
 - business developers
 - quasi-public entities
 - regional non-profits
 - housing developers
 - homeless providers
 - city/town personnel
 - boards, professional organizations
 - other state agencies

Destruction of PII

Destroy PII When No Longer Needed

<u>Before</u> Destruction Consider the Following:

- Active Litigation Hold (confirm with EOHED Office of General Counsel)
- Record Retention
 Requirements (click <u>here</u>
 for schedule)

Methods of Destruction

Use Proper Destruction Methods Including:

- Cross-shredding or secure containers for paper documents
- Proper, secure destruction of electronic files and equipment hard drives (contact IT for assistance)

Serious Consequences Arise from Unauthorized Use or Access of PII



Massachusetts Law creates specific duties for the owners/users of information that tie a person to information that might be considered private

First Step IF There is a Breach

In the event of a breach or loss of data/equipment:

DO:

Immediately Notify EOHED's
INFORMATION SECURITY OFFICER
OR
General Counsel

DO NOT:

Ignore It

Hide It

Wait

Examples of Risk Severity

Perceived Risk	Severity	Mitigation Tactic
You are taking over the function(s) from a predecessor and his/her files contain old files with Social Security Numbers.	High	Alert the Office of General Counsel or the HR Director to determine how to handle the files. Do not destroy or move first.
You require data or information about a		Collect minimum quantity only.
particular program, agency etc., and your request is not specific as to what you need and you are sent personnel files in the package.	High	If you do not need the information, do not ask for it.
You are creating a database or data set that contains PII.	High	Only access information necessary for the proper performance of your job; speak with the IT Director determine appropriate access controls.
You are leaving for the night and you do not shut down your computer or put away the information on your desk because you will be back in the morning.	Moderate	Securely store and protect PII against unauthorized access, destruction, use, modification, disclosure and loss.
You receive a request for Personal Information outside of the normal course of program management.	Moderate	Escalate the request to the Information Security Officer (ISO) Officer or General Counsel before responding.
Unauthorized people seek Personal Information from you or your means to access it.	Low	Beware of unauthorized people and requests. Do NOT share or disclose passwords. Disclose PII only on a NEED-TO-KNOW basis.

EOHED Information Security Program Goals

COLLECT

The minimum quantity of Personal Information reasonably needed to accomplish legitimate purpose for which information is being collected.

IMPLEMENT

The maximum feasible measures reasonably needed to ensure the security, confidentiality, and integrity of Personal Information.

SECURELY STORE

And protect Personal Information against unauthorized access, destruction, modification, disclosure, and loss.

DO NOT DISCLOSE

Personal Information and data except on a need-to-know basis.

DESTROY

Personal Information and Data as soon as it is no longer needed or required to be maintained under state or federal law.

COMPLY

With the Agency's administrative, technical, and physical safeguards for Personal Information.

With relevant federal and state *privacy and security* laws and regulations.

Examples of What Governs How EOHED Protects PII

State and Federal Statutes on Privacy and Security

- FIPA
- Public Records Laws
- Security Breach Laws
- Privacy Laws

PROTECTING PII

Executive Orders, Contracts, Policies, Standards and Guidelines

- EO 504
- Contracts between the Agency and Data Providers
- ITD Security Policies, Standards and Guidelines
- EOHED-specific Security Policies, Standards and Guidelines

Conclusion

1. YOU Are responsible for identifying and safeguarding PII.

2. THINK Before accessing or transmitting PII.

DO NOT

Any PII to or from anyone outside of appropriate

RELEASE OR agency personnel without first vetting it through an internal process (i.e., contact EOHED ISO or GC).

4. ESCALATEQuestions about what PII is to the EOHED ISO, GC, or IT Director.

CONFIRMATION OF TRAINING ATTENDANCE

The Executive Order 504 - Personal Information Security Training session has now concluded; click the icon to submit your name as confirmation of your completion of this training session.



ANY QUESTIONS? ASK:

- DHCD General Counsel
 - Roberta Rubin
 - 617-573-1505
- DHCD Information Security Officer
 - Susan Terrey
 - 617-573-1103
- DHCD Information Technology Director
 - Tom Cream
 - 617-573-1283