IDENTIFYING AND SAFEGUARDING PERSONAL INFORMATION - TRAINING

Department of Housing and Community Development

2018

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 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.
 - Lock computer when away from desk, lock away portable devices

Information Security Program

□Goal of Information Security Program:

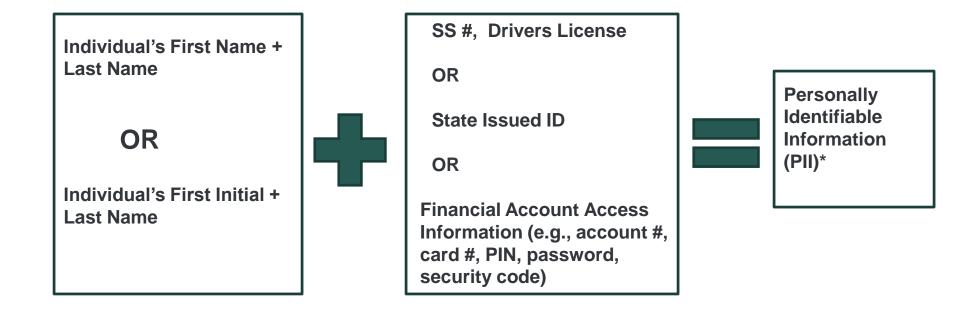
Adopt and implement the maximum feasible measures reasonably needed to ensure the security, confidentiality and integrity of Personal Information.

□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.
- Disclose Personal Information and data only 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.

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







Name			Today's Date://
Address:		-	Photes
Cier		Zipi	Work Phone
Goardian (If Applicable):			Outputon
thirth Duor.	Social Security A		/ Last Evy Engry / /
Name of Medical Doone:			De's Women
THE STORAGE PARTY.			Last Matrol Faure / /
Medical History Do you have any allogue to medican-	au One Op	e li jus, sa	
List are moderation for the (orline)	of our commoder	cen, seperat, o	nor the country medications and bonse remedies;
		Day I	
List of major injuries, surgestes and/or	boarished on v	And water	
the second of select selection and or			
List esp of the following that you have			
List are of the following that you have age inflations or eye injury:			
List any of the following that you have upo inflations or eye injury: Are you program and/or maning:	halt amount eyes.	lary sys., driv	
Last any of the following that you have eye infloations or eye injury: Are you prognant and/or maning? (Do you wear glasses) Do you were consect lesses?	Jan Dyes Day Dyes H Day Dyes H	pay, how old yes, how old	oping cycles, prominent syns, gleazurus, retired disease, ea la year promini juar of kroses) is juar processi pair of kroses)
Last any of the following that you have eye infloations or eye injury: Are you prognant and/or maning? (Do you wear glasses) Do you were consect lesses?	Jan Dyes Day Dyes II Day Dyes II	pay, how old yes, how old	oping eyeld, prominent eyes, gleaverus, retired disease, car is your present pair of lemes)
Last any of the following that you have up in infasts on or sylvings: Are you program and/or namings Do you were glassed Do you were conset lessess Type of contact house: Type of contact house:	Jan Dyes Day Dyes II Day Dyes II	pay, how old yes, how old	oping cycles, promunent syon, gloscome, retired disease, car le year present pair of kroses' 10 year present pair of kroses'
Last any of the following that you have eye infactions or eye tripery: Are you prognant and/or naming: Do you were connect letters? Fruits History Fruits History	Dan Dyes Dan Dyes H Dan Dyes H Soft Differentes	per, how old yes, how old yes, how old	oping world, prominent syon, gloverme, retind disease, or is your present pair of knowle is your present pair of knowle that Ass they confortable Tyes Two
Last any of the following that you have eye infactions or eye tripery: Are you prognant and/or naming: Do you were connect letters? Fruits History Fruits History	Dan Dyes Dan Dyes H Dan Dyes H Soft Differentes	per, how old yes, how old yes, how old	oping cycles, promunent syon, gloscome, retired disease, car le year present pair of kroses' 10 year present pair of kroses'
Last any of the following that you have got infections or nys trigery. Are, you prognant and/or naming: Do you were glossed Do you were consect thresses Type of contact house: Type of contact house: Dispute ones are family bloomy pureau, DISEASE/CONDITION	Dad immed eye. Das Dyes Das Dyes If Das Oyes If Soft D Extender NO VES	per, how old yes, how old yes, how old	oping cooks, prominent syns, pleasures, retind disease, or je more present pair of breach lyse of prominent of breach there has they comfortable at the more children for the believing conditions
List any uf the fild/reing that you have got infection or not injury. Are you prognant and/or namings: Do you want glossed: Do you were consist lenses: Tigs of contact hines: Family Hinory Family Honory	balt municipal. Day Dyes Day Dyes 16 Day Dyes 16 Soit Diamades	per how old yes, how old 100 mm D t	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
Lot up of the fidewing that you have up arteriors or specificary. Are you prognet and for assumpt for the your weer glasses of the Do you were glasses for Type of contact know. If Rigid. If Parally History. Passes now see faculty housey quarters. DISEASE!/CONDITION BEASE!/CONDITION	Dad mond eye. Das Dyes Das Dyes If Soft Dismede NO YES D D	per, how old yes, how old yes, how old	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List asy of the fi-Dreing that you have epo infections or eye infect. As you prepare and/or assuming: Do you were glassics. Do you were connect tension: Do you were connect tension: Princip of contact home: Princip of contact home: Princip of fine you from you for your your your your your your your yo	Date Dyes Date Dyes Date Dyes Date Dyes Date Dyes Date Dotter Dot	yes, how old yes, how old I West Dis	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
Lor ary of the GArring that you have type relations or excitatey. As you prepared with or namely of Says in ware justed. Says in ware content feature. The property of content have content feature. The property of content have been partially Family History. See note was feature have partially Says note was feature have partially Content. Conten	had around eyes. Day Dyes 10 Day Oyes 16 Son Diamake NO VIS D D D D D D D D D D D D D D D D D D D	pro tos elli pro tos elli pro, tos elli l West D S logo, shidox	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List asy of the fi-Dreing flat you have epo infestions or synthesis. As you proposed and/or assuming: Do you were glassically to be proposed to be propose	Date Dyes Date Dyes Date Dyes III Soft Distribution of the No VES	per tree elli	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
Lor ary of the GArring that you have type relations or excitatey. As you prepared with or namely of Says in ware justed. Says in ware content feature. The property of content have content feature. The property of content have been partially Family History. See note was feature have partially Says note was feature have partially Content. Conten	Dask trouvil eyes. Das Oyes to Das Oyes to Son O'Estander NO VES	per tour ald yes, bore old lives and	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List are of the IGA resignation was have go in a facilities on a consistent of the	Dask promid eyes. One Oyes II One Oyes II See O'Emnake NO VIS O O O O O O O O O O O O O O O O O O O	per true elli	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List are of the IGA resig that you have got selection or epiciety. Any you present only to the resigned to you you present of the young present of the youn	bad moral eye. One Oyee If One Oyee If Soit Olimnike NO VES	Jan ope, done	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List are of the It-Desiring this was have rep relations on excitage, the copy reputer and or average. Do you were connect times? Do you were connect times? Dipt of connect home. DEQU. Dipt of connect home. DEQU. Dipt of connect home. DEQU. Dipt of Connect home. DEQU. DIPLOSE (COUNTION HIM.) Himsels. Connect times of the connect has a connect to Mendre Department of Mendre Department	had smooth epoc. Doe Does Does Does Does Does Does	per troy of the per troy of th	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List are of the fidewing this year bare on principles or spirities, we spirities out the principles of	hadt treoud eyes. Just Dyes Jus	per tros old yes, tros old West Dis	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
List are of the It-Desiring this was have rep relations on excitage, the copy reputer and or average. Do you were connect times? Do you were connect times? Dipt of connect home. DEQU. Dipt of connect home. DEQU. Dipt of connect home. DEQU. Dipt of Connect home. DEQU. DIPLOSE (COUNTION HIM.) Himsels. Connect times of the connect has a connect to Mendre Department of Mendre Department	had treend eyes. One Days One Days	Jan eye, dree ell yes, troe ell 18 cm - Di Di Di Di Di Di Di Di Di Di Di Di Di D	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
Last are of the fi-Aresing-this year bare- gravitations on rejetiety. Any year passes and rejetiety. Any year passes and year passes Doys was content to come of the passes Type of course home. If Eggl of Type of course home. If Eggl of the passes have the passes of th	hali monul epo. Jun Dyn Hon Hon Dyn Dyn Dyn Dyn Dyn Dyn Dyn Dyn Dyn Dy	per toward per toward (West Dis	oping gracks, prominent syns, plearum, retined disease, on in our present pair of braced by the open pair of braced they are the synthesizable of year of su ghistograr decembly for the believing conditions
Lie ary of the Glavesing this year large spiriteries or spiritery. Any year pages and on earning it was year pages and on earning it was year pages and on a ready if year year. He was a ready of the page of years, he was a BERGARI/CONDITION Blakes Corner to the page of years when years are year years of Glaveson and year years of Glaveson. Glaveson Manda Department Disasses and Manda Department Disasses and Glaveson Black Department of Glaveson	had treend eyes. One Days One Days	Jan eye, dree ell yes, troe ell 18 cm - Di Di Di Di Di Di Di Di Di Di Di Di Di D	oping cooks, prominent syns, pleasures, retind disease, or je more present pair of breach lyse of prominent of breach there has they comfortable at the more children for the believing conditions

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

PII may be physical, electronic or verbal

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.

Physically Protect PII Using a Clean Desk / Clean Screen Policy

Establish a culture of security and trust.

- A clean desk can produce a positive image when our business partners visit the agency.
- Reduce the threat of a security incident as confidential information will be locked away when unattended.
- Sensitive documents left in the open can be stolen by a malicious entity.
- Sensitive working papers are expected to be placed in locked drawers/cabinets.
- Consider scanning paper items and filing them electronically.
- Use shredding/secure destruction bins for sensitive paper documents when they are no longer needed.
- Lock your desk and filing cabinets at the end of the day.
- Lock your computer screen when you leave your desk for an extended period or if someone is in your office unattended.
- Log off your computer when you leave your desk at the end of the work day.
- Lock away portable computing devices such as laptops or PDA devices.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

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.

Destruction of PII

Destroy PII When No Longer Needed

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

- Active Litigation Hold (confirm with Legal/General Counsel)
- Record Retention Requirements

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

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 the Executive Director
OR
Legal/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 Legal/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 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	Collect minimum quantity only. 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 Executive Director to 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 Executive Director or Legal/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.

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.

Conclusion

1. YOU Are responsible for identifying and safeguarding PII.

2. THINK Before accessing or transmitting PII.

DO NOT

3. RELEASE OR

ACCEPT

Any PII to or from anyone outside of appropriate agency personnel without first vetting it through an internal process (i.e., contact Executive Director or Legal/General Counsel)

Questions about what PII is to Executive Director or **4. ESCALATE**Legal/General Counsel or DHCD Management contact(s).