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

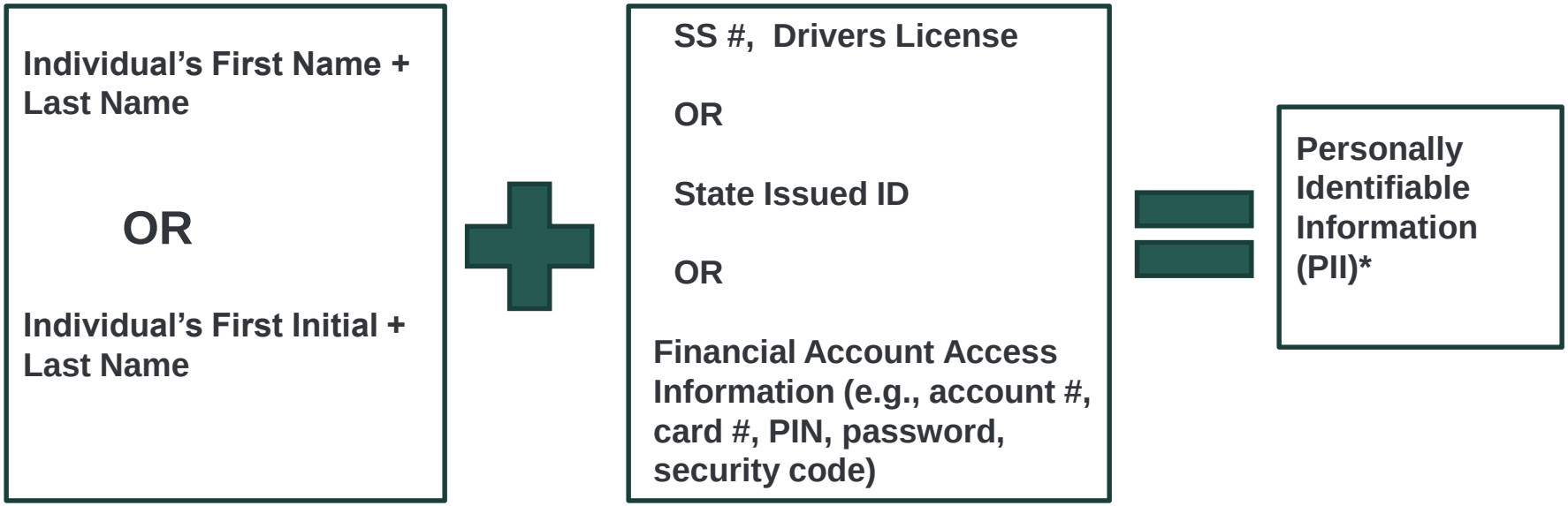
- Goal of Information Security Program:

  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**

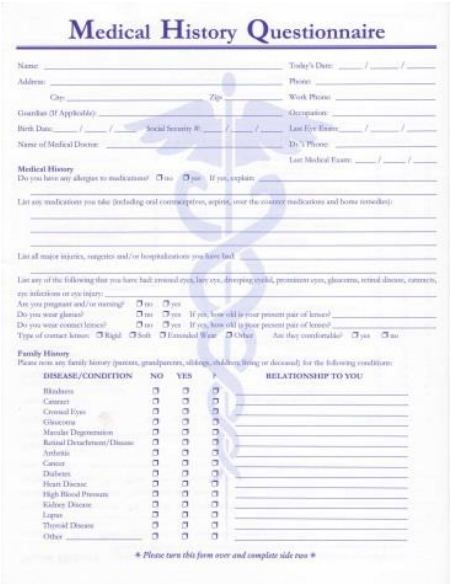
+

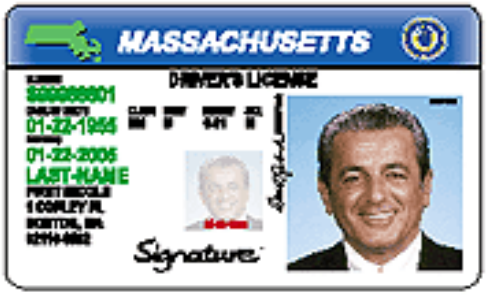
Can be readily associated with a particular individual

=

Personal Data

Examples of PII





What PII is NOT:

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

- ✓ **Intelligence information, evaluative information,**

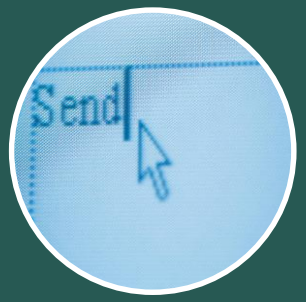
OR

- ✓ **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

- 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 non-authorized 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 acknowledge-ment.

- 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

Before *Destruction Consider the Following:*

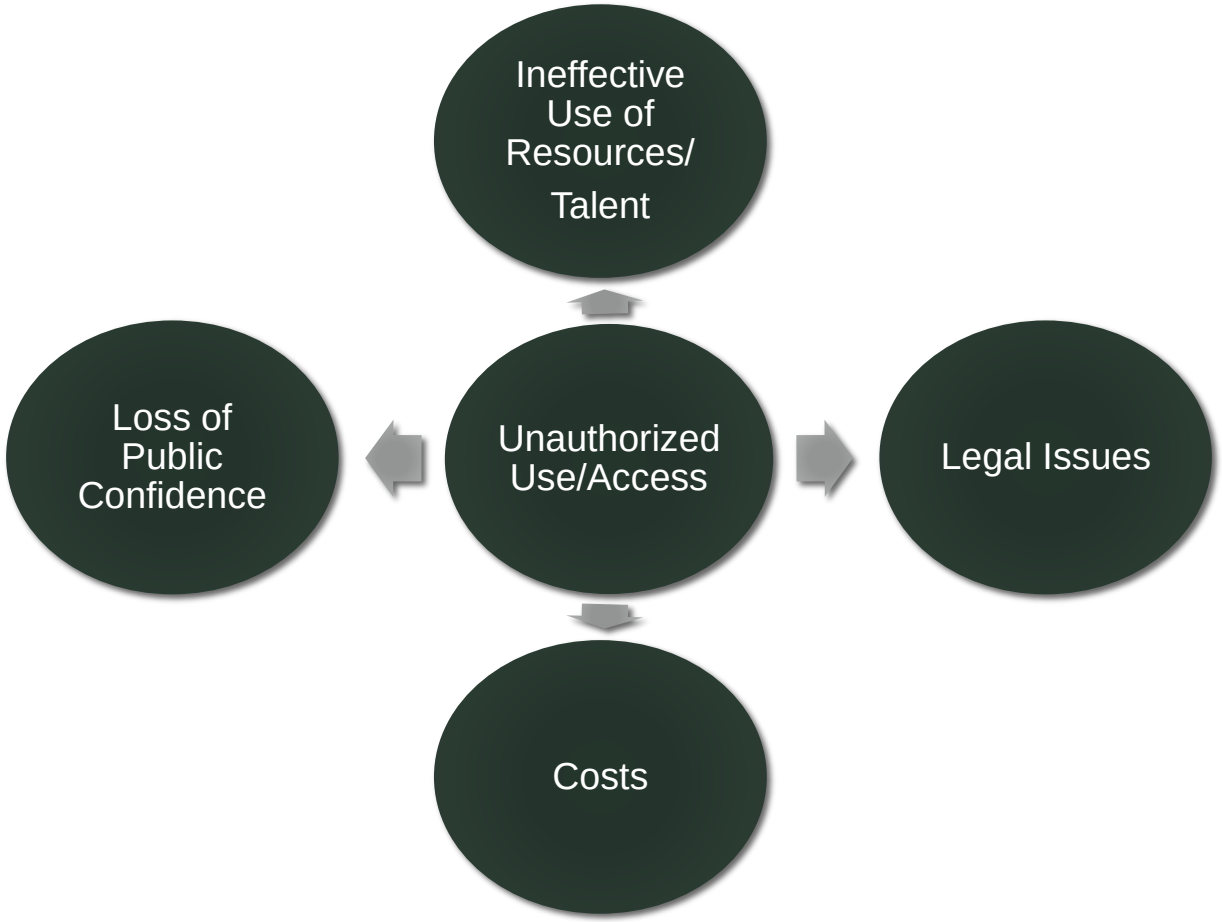
- Active Litigation Hold (confirm with Legal/General Counsel)
- Record Retention Requirements

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

Acting quickly and notifying the appropriate people may help mitigate the damage

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.
3.	**DO NOT 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)
4.	**ESCALATE**	Questions about what PII is to Executive Director or Legal/General Counsel or DHCD Management contact(s).