

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

- | | | |
|----------|--|---|
| 1 | Introduction | This training is a requirement pursuant to Executive Order 504 |
| 2 | Identifying Personal Information | What, when, and where to identify Personal Information |
| 3 | Safeguarding Personal Information | How to safeguard Personal Information |
| 4 | EOHED and Legal Underpinnings | Why you are required to safeguard Personal Information |
| 5 | 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):

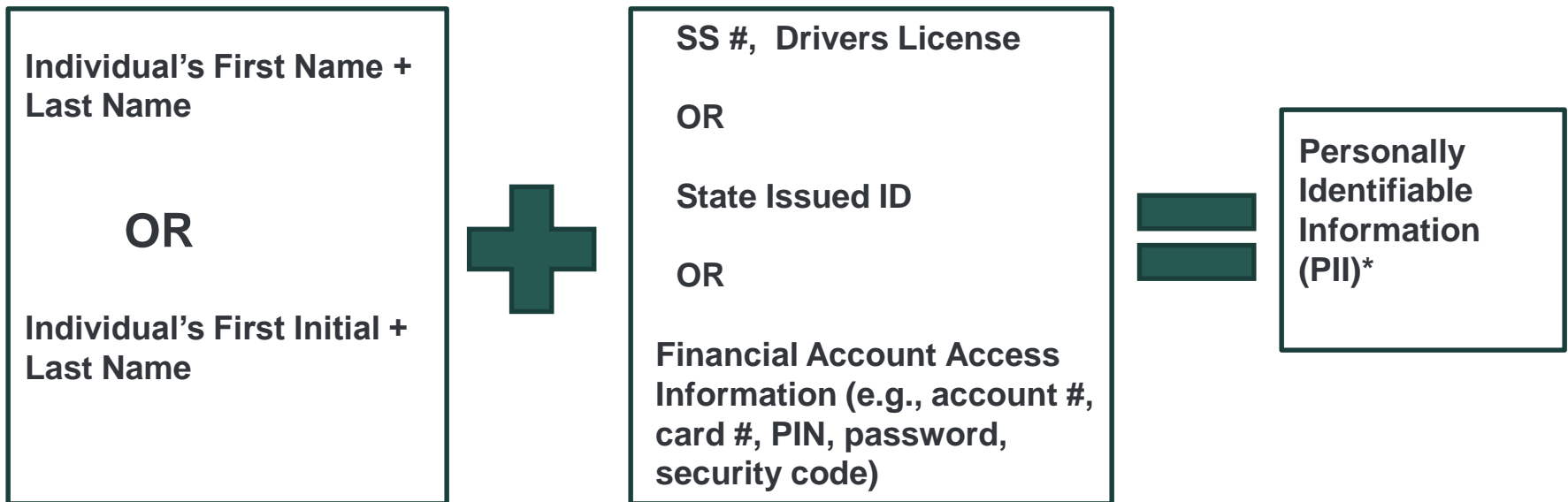
Adopt and implement the maximum feasible measures reasonably needed to ensure the security, confidentiality and integrity of Personal Information.

□ 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.
- 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

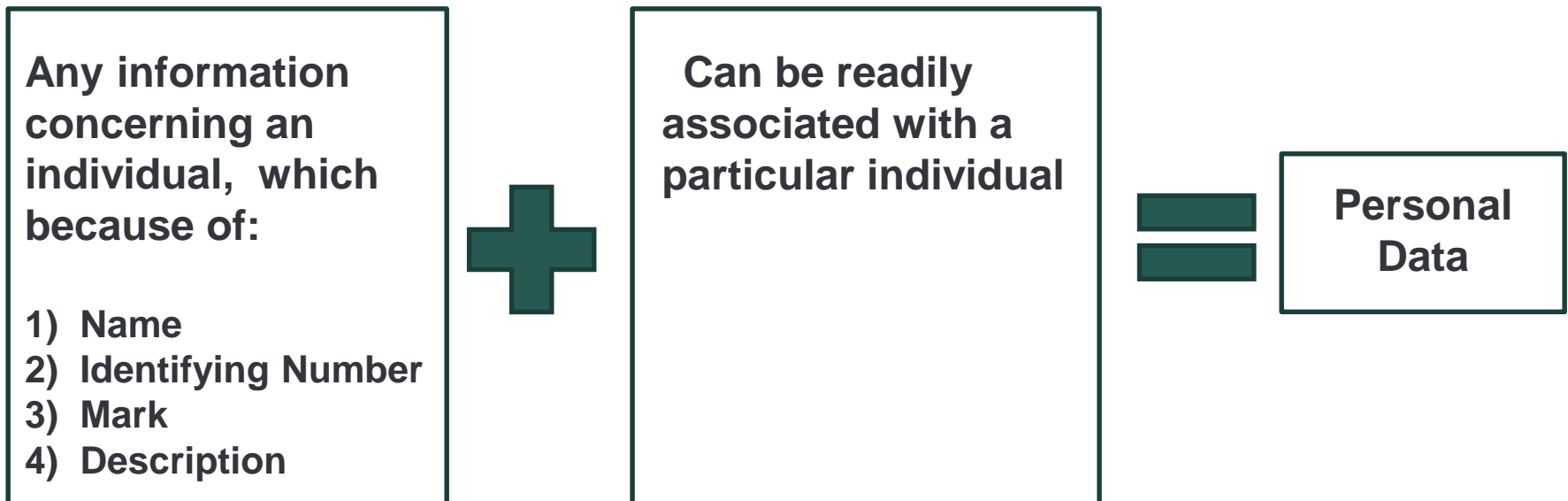
(as defined by M.G.L. c. 93H, § 1)



*Throughout this training, we will use "PII," the universally accepted acronym for **Personally Identifiable Information**, which means the same as Personal Information.

Personal Data

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



Examples of PII



Medical History Questionnaire

Name: _____ Today's Date: ____/____/____
 Address: _____ Phone: _____
 City: _____ Zip: _____ Work Phone: _____
 Guardian (If Applicable) _____ Occupation: _____
 Birth Date: _____ Social Security #: _____ Last Eye Exam: ____/____/____
 Name of Medical Doctor: _____ Dr.'s Phone: _____
 Last Medical Exam: ____/____/____

Medical History
 Do you have any allergies to medications? no yes. If yes, explain: _____
 List any medications you take (including oral contraceptives, aspirin, over the counter medications and home remedies): _____

 List all major injuries, surgeries and/or hospitalizations you have had: _____

 List any of the following that you have had (stroke, eye, leg, eye, sleeping, cough, persistent pain, phlebotomy, retinal disease, cancer, eye infection or eye injury): _____
 Are you pregnant and/or nursing? no yes
 Do you wear glasses? no yes. If yes, how old is your present pair of lenses?
 Do you wear contact lenses? no yes. If yes, how old is your present pair of lenses?
 Type of contact lenses: Rigid Soft Extended Wear Other. Are they comfortable? yes no

Family History
 Please check any family history (parents, grandparents, siblings, children living or deceased) for the following conditions:

| DISEASE/CONDITION | NO | YES | RELATIONSHIP TO YOU: |
|---------------------------|--------------------------|--------------------------|----------------------|
| Blindness | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Cancer | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Coronary Artery Disease | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Glaucoma | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Muscle Degeneration | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Renal Dysfunction/Disease | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Schizophrenia | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Stroke | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Tuberculosis | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| High Blood Pressure | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Kidney Disease | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Leprosy | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Thyroid Disease | <input type="checkbox"/> | <input type="checkbox"/> | _____ |
| Other | <input type="checkbox"/> | <input type="checkbox"/> | _____ |

* Please turn this form over and complete side two *



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).**

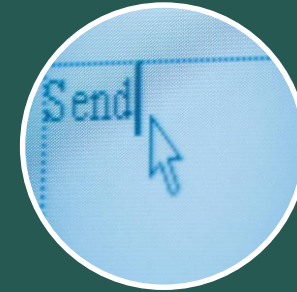
Where PII May “Live”



- 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.**

Safeguarding PII

Collect Minimum Quantity

- 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.

Disclose PII only on a NEED-TO-KNOW basis

- 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 Data Exchange Acknowledgement

- Complete it if data is sent outside.
- Contact EOHED Information Security Officer for a copy of the acknowledgement.

Protect Your Passwords

- 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

Before Destruction Consider the Following:

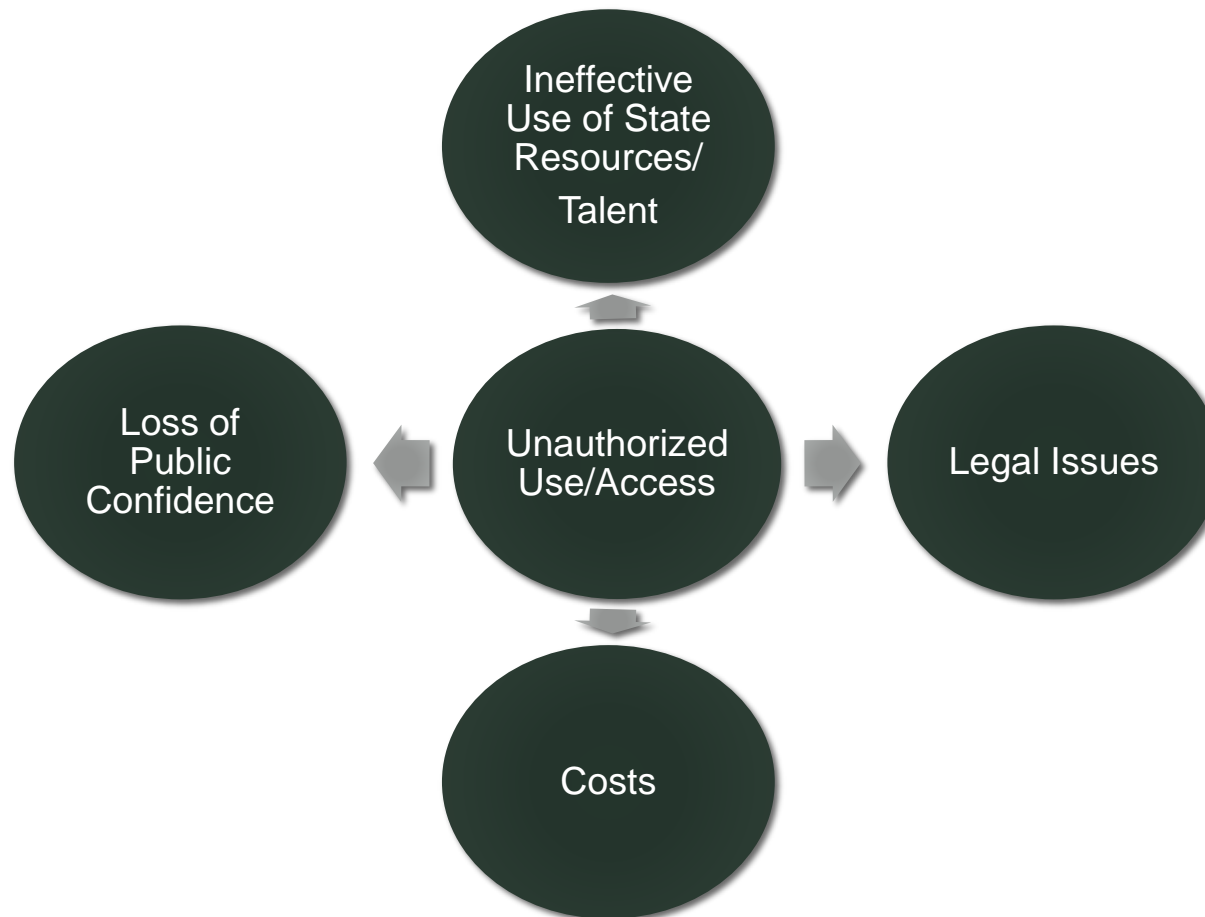
- Active Litigation Hold
(confirm with EOHED Office of General Counsel)
- Record Retention Requirements (click [here](#) for schedule)

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

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 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 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 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

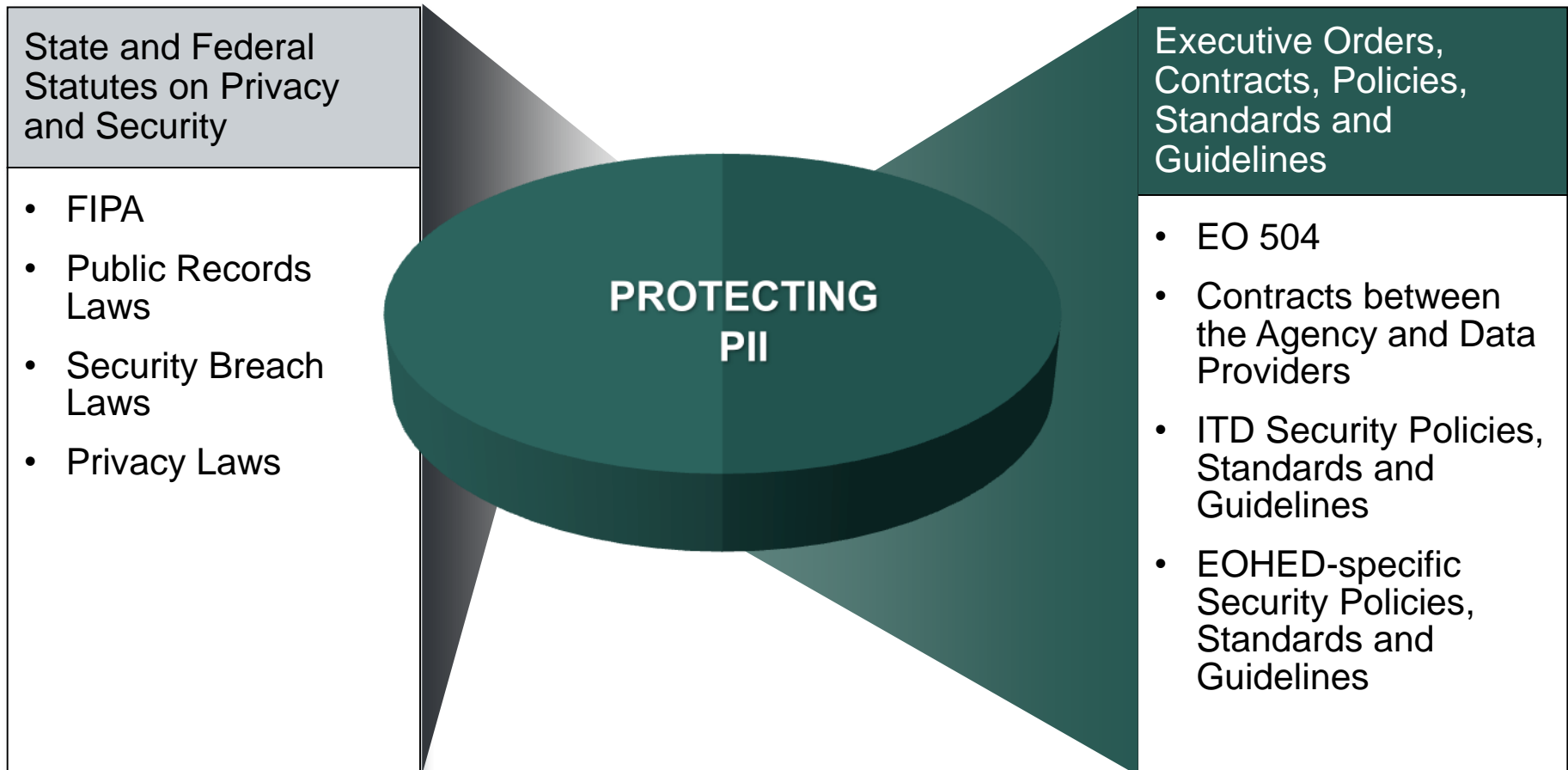
Personal Information and Data as soon as it is no longer needed or required to be maintained under state or federal law.

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



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 EOHED ISO or GC).
- 4. ESCALATE** Questions 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