





How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC



**How to Identify, Maintain, and Safeguard
Personal Information**

**Barbara Phillips, PERAC General Counsel
Derek Moitoso, PERAC Associate General Counsel**




**Statutory and Regulatory
Security Requirements**

- **Fair Information Practices Act (FIPA) G.L. 66A**
 - In general, FIPA creates a non-disclosure requirement of personal data when such information is not subject to disclosure.
- **G.L. 93H – Security Breaches**
 - Triggering events require holders to provide notice in the event of unauthorized access or use of personal information.
 - Holders must protect personal information.
- **201 CMR 17.00 Office of Consumer Affairs and Business Regulation**
 - Municipalities exempt from rigorous procedures, but must provide information on losses of personal data. Regulations offer good guidance.


5/16/10 2

How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC




Safeguarding Personal Information




- **Identity theft is a serious crime**
- **Recent promulgation of laws to protect against identity theft**
- **Importance of developing and implementing:**
 - uniform policies and standards
 - to safeguard the security, confidentiality, and integrity of personal information
- **Written information, security policies governing collection, use, dissemination, storage, retention and destruction of personal information are recommended**
- **Periodic Training for all employees, including contractors, recommended**
- **Consider conducting a self-audit periodically**

5/16/10 3



Safeguarding Personal Information




- **Consequences of unauthorized use or access of personal information**
 - Identity theft
 - Other unplanned costs (to data subject and to the agency)
 - Staff downtime
 - Loss of public confidence
 - Legal issues


5/16/10 4

How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC




What Is Personal Information?




- **Personal information (G.L. c. 93H) is defined as:**
 - A *resident's* first name + last name or first initial and last name
 - in combination with any 1 or more of the following:
 - Social security number;
 - Drivers license (or state issued i.d.) number; or
 - Financial account number

- **Personal Data (under Fair Information Practices Act (FIPA)) is defined as:**
 - Any information concerning an individual which because of:
 - Name,
 - Identifying number,
 - Mark, or
 - Description
 - Can be readily associated with a particular individual
 - Except for information:
 - Contained in a public record (see G.L. c. 4 § 7(26));
 - Intelligence information, evaluative information; or criminal record information (as defined in G.L. c. 6 § 167), which shall be governed by the Criminal Offender Record Information (CORI) Act.

5/16/10 5



Examples of Personal Information




- **Tax Information**
- **Credit Card Information**
- **Account Information**
- **Banking Information**
- **Addresses and Telephone Numbers**
- **Name and Social Security Number**
- **Health Record Information**


5/16/10 6

How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC



Ways to Store or Transmit Personal Information




(1) Hardcopy paper

- What
 - Reports
 - Letters
 - Faxes
 - Printouts
 - Memos
 - Notepads
 - Sticky notes
- Where
 - File cabinets
 - Desks
 - Printers or Faxes
 - On his or her person


(2) Oral

- Over the phone
- In meetings
- With members/employers

5/16/10 7



Ways to Store or Transmit Personal Information (cont'd)




(3) Electronic records

- Electronic Handheld Devices: PDAs, Blackberries, cell-phones, flash-drives, CD/DVDs, floppy disks.
- Possible Board Systems:
 - Email and Voice-mail
 - Copiers & Facsimile Machines
 - Production and Development databases
 - Files stored on individual PC/laptop or on network drives
 - Servers on site or at remote host
 - System and database logs
 - Reserved Equipment in storage area
 - Backup tapes onsite or offsite
 - Examples of Board records that collect or use Personal Information
 - Disability application
 - Calculation
 - Payment information
 - Membership information
 - Contribution information


5/16/10 8

How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC




Maintain and Safeguard Personal Information




- **Collect minimum quantity**
 - if you don't need it, don't ask for it
 - reconsider your current processes
 - only access information necessary for the proper performance of your job

- **Disclose personal information on a need to know basis**
 - If you receive a request for personal information outside the normal course of program management, the request must be reviewed and approved by the staff person designated to release information.
 - Beware of non-authorized people seeking information or means to access personal information.
 - Phishing (illegitimate email requests for information),
 - Impersonation (as agency IT staff via email, over the phone),
 - Shoulder surfing (looking over your shoulder while you use your computer)

5/16/10 9



Maintain and Safeguard Personal Information




- **Destroy personal information when no longer needed**
 - Consider the following before destroying any record
 - Active litigation holds
 - Records retention requirements for certain programs (e.g. under HIPAA)
 - Records in Common Schedule

- **Methods of Destruction**
 - Shredding paper or documents that contain personal information
 - Electronic information (computers, handheld devices); ensure proper deletion of files (e.g. special deletion protocols of storage media)


5/16/10 10

How to Identify, Maintain and Safeguard Personal Information

Barbara Phillips and Derek Moitoso, PERAC




Maintain and Safeguard Personal Information




- **Physical Protection of Personal Information (PERAC's protocol as an example)**
 - Reception Desk – Visitors sign in and are accompanied by employee or are issued a temporary Visitor's Badge.
 - Access I.D.: Access cards are provided to employees of PERAC with designated access hours. The four access doors remain locked at all times.
 - Door Alarms: Employees are provided with access codes to arm and disarm the office areas.
 - Lock file cabinets in offices containing personal information
 - Do not leave personal information unattended in non-secure environment (on desk, in communal meeting space, on sticky note, at printer or fax machine etc.)
 - Keep secure spaces secure (don't prop open locked doors or let in others that don't have authorized entry).
- **Oral dissemination of personal information**
 - Only discuss when appropriate (while performing job function).
 - Do not discuss personal information in non-private spaces (e.g. elevators, cubicles etc.)

5/16/10 11



Procedural Methods to Safeguard Information





- **Example of an Acceptable Use Policy**
 - Do not access or disseminate personal information unless required by your job
 - Never share passwords
 - Promptly notify your supervisor if you suspect password has been compromised
 - Log off or lock desktop when you step away from your computer
 - E-mail messages that contain personal or confidential information must be encrypted
- **Comply with specific system user account requirements (use strong passwords, don't use somebody else's password or i.d.)**
- **Use resources appropriately: Do not store personal information on mobile devices (e.g. laptops, flash drives, CD/DVD, phones, etc.) or in non-secure applications (e.g. typical email or other desktop applications e.g. MS Excel) unless the data is encrypted.**

5/16/10 12

How to Identify, Maintain and Safeguard Personal Information



Barbara Phillips and Derek Moitoso, PERAC



Board Specific Policies and Guidelines

- **Information Technology Acceptable Use Policy Should:**
 - Encourage the use of IT Resources (ITR) to deliver better and lower cost services, with the understanding that users will refrain from using ITR for unacceptable purposes and with no expectation of privacy.
 - Prohibit ITR from being used to access and disseminate any confidential or personal information that is not a job requirement.
 - Prohibit personal or medical information from being included in e-mail message text and any attachments containing personal or medical information must be encrypted.
- **Confidentiality and Information Security Agreements**
Acknowledged and signed by all employees and contractors

5/16/10 13



Conclusion

- **Everyone is responsible for safeguarding personal information**
- **Think before accessing or transmitting personal information**
 - Treat all personal information as if it was your own information.
- **Do not release any personal information to anyone outside the appropriate Board personnel without first vetting it through internal process:**
 - Check with your supervisor or review Board policy.
 - Legal review may be necessary (subpoenas, rfps, public records requests, data subject requests).
 - Follow all Board privacy and security policies (maintain the safety and security of your systems).

5/16/10 14