Attachment B

Public Health
Seattle & King County

Department Policies

Title	Document Code No.
Identity Theft Prevention Program	INF 2-3 (DPH DP)
Department/Issuing Agency	**Effective Date.**
Public Health – Seattle & King County	October 30, 2009
Approved	DPH Director

1.0 SUBJECT TITLE: Identity Theft Prevention Program

1.1 EFFECTIVE DATE: October 30, 2009

1.2 TYPE OF ACTION: New

1.3 KEY WORDS: Fraud, Identity, Red Flags

2.0 PURPOSE:

To establish an identity theft prevention program that meets the requirements of the Federal Trade Commission's (FTC) Red Flags Rules mandated by 16 CFR § 681.1.

3.0 ORGANIZATIONS AFFECTED:

Applicable to the Department of Public Health Seattle-King County (PHSKC).

4.0 REFERENCES

4.1 Fair and Accurate Credit Transactions Act of 2003 (FACTA)

4.2 16 CFR § 681.1 – Federal Trade Commission, Identity Theft Rules

4.3 45 CFR Part 164 – Health Insurance Portability and Accountability Act

4.4 RCW 9.35.020 – Identity Theft

4.5 RCW 19.182 – Washington Fair Credit Reporting Act

5.0 DEFINITIONS:

5.1 "Fraud" means an intentional deception made for personal gain or to damage another individual.

5.2 "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including

5.2.1 Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, medical coupon/card, employer or taxpayer identification number, credit card number;

5.2.2 Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

5.2.3 Unique electronic identification number, address, or routing code; or

5.2.4 Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

5.3 "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

5.3.1 "Medical Identity Theft" means the use of a person's name and/or other parts of their identity without the person's knowledge or consent to obtain medical services or goods. Medical identity theft also occurs when an individual uses another person's identity to submit false claims for medical services and falsifying medical records to support those claims.

5.4 "Mitigation" means activities designed to lessen the severity or intensity of damage created by identity theft.

5.5 "Red Flags" means potential patterns, practices, or specific activities indicating the possibility of identity theft.

5.6 "Red Flags Rule" means the FTC rule that requires a written Identity Theft Prevention Program designed to detect the red flags of identity theft, take steps to prevent the crime, and to mitigate damage from identity theft.

5.7 "Safeguards" means precautionary activities to protect identifying information.

5.8 "Workforce" means employees, volunteers, trainees, and other persons in Public Health whose conduct, in the performance of work, is under the direct control of Public Health, whether or not they are paid by Public Health. Workforce includes, but is not limited to, other categories of persons including contract employees, students, and work study students/interns.

6.0 POLICIES:

6.1 PHSKC will maintain and administer an Identity Theft Prevention Program in order to detect, prevent, and mitigate financial and medical identity theft.

6.2 The Chief Financial Officer (CFO) is the chief official for this policy and is responsible for the administration and maintenance of the policy.

6.3 All managers/supervisors will assess transactional systems and processes that contain personal identifying information that may present opportunities for identity theft.

6.3.1 The assessment will identify potential red flags using Appendix 9.1, Indicators of Potential Identity Theft Red Flags.

6.3.2 When the red flags are identified, determine actions that can be taken to eliminate or reduce identity theft.

6.3.3 This assessment will be documented on the Red Flag Assessment Form (Appendix 9.2) and will be conducted whenever a transactional system or process is added, deleted, or modified.

6.3.3.1 If a manager/supervisor believes that a system or process is of minimal risk, not requiring red flag identification he/she shall provide the basis of this to the CFO who will make the final determination of red flag designation.

6.3.4 The results of the assessment will be provided to the CFO.

6.4 The workforce will be trained on this policy and operational procedures upon initial employment with the department and additionally as needed.

6.5 The workforce will be trained to look for red flags that may indicate the potential for identity theft. To detect red flags, the workforce should use alternative information to verify identity such as:

- Driver's license, passport, or other photo identification
- Social Security Number
- Date of birth
- Residence address and telephone number
- Insurance card (if available)
- Other identifying information (i.e. challenge questions, library card, utility bill, etc.)

6.5.1 When a workforce member discovers a red flag, he/she shall report this to their supervisor immediately.

6.6 Whenever an attempted or actual identity theft is reported, the supervisor will immediately report the incident by phone to the Compliance Office, who shall notify the CFO. The supervisor will follow up with a written incident/accident report.

6.7 When identity theft is reported, a mitigation plan that has a strong focus on helping the victims of this crime will be developed. Mitigation strategies may include:

- Monitoring for evidence of identity theft;
- Contacting the client;
- Changing any passwords, security codes, or other security devices that permit access to personal information; and
- Notifying law enforcement.

6.8 Managers/supervisors will evaluate ways to reduce potential identity theft through internal safeguards and practices. For example, limiting the use of a social security number, not photocopying documents unless necessary, ensuring that credit card and bank account numbers are appropriately safeguarded, etc.

6.9 This policy shall be reviewed at least annually.

7.0 PROCEDURES:

Action By: Managers/Supervisors

Action:

7.1 Assess all transactional systems and processes for identifying information.

7.2 Identify potential red flags of identity theft for the system or process.

7.3 Provide the results of the assessment to the CFO.

7.4 Ensure the workforce is trained on this policy and operational procedures to prevent identity theft.

Action By: Workforce

Action:

7.5 Know the red flags for potential identity theft.

7.6 Be alert for potential patterns, practices, or specific activities indicating the possibility of identity theft. Immediately report attempted or actual identity theft to the supervisor.

Action By: Supervisor/Division Manager

Action:

7.7 Immediately report any attempted or actual identity theft to the Compliance Office by phone, followed up with an incident/accident report.

Action By: Compliance Office

Action:

7.8 Notify the CFO when receiving a report of attempted or actual identity theft.

Action By: Chief Finance Officer

Action:

7.9 Review all evaluations of transactional systems and processes.

7.10 Review all reports of attempted or actual theft of identifying information and take appropriate action.

8.0 RESPONSIBILITIES:

8.1 Managers/supervisors are responsible for identifying transactional systems and processes for identifying information, determine red flags for these systems/transactions, and training the workforce on this policy and operational procedures to prevent identity theft. They will also immediately report to the Compliance Office any attempted or actual identity theft.

8.2 The workforce is responsible for being alert for red flags or suspicious activity in transactional systems and processes and reporting this to their manager/supervisor.

8.3 The CFO is responsible for reviewing all evaluations of transactional systems and processes and reviewing reports of attempted or actual identity theft and determining appropriate corrective actions to be taken.

9.0 APPENDICES:

9.1 Indicators of Potential Identity Theft

9.2 Red Flag Assessment Form

Policy Owner	Last Review Date	Comments
CFO		Established