



Policy 26.01
Version Number: 2

Initial Approved Date: December 15, 2006
Last Modification Date: March 17, 2008

TO:

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM:

Director of Health

SUBJECT:

Notification of Security Breaches.

SCOPE:

Department of Health – All Programs

PURPOSE:

To decrease the risks of identity theft by establishing Department of Health (“DOH”) security breach notification and reporting policies and guidelines requiring the notification of an individual(s) whenever the individual’s personal information has been compromised by unauthorized disclosure, and to comply with the requirements of Hawaii Revised Statutes (“HRS”) Chapter 487N.

POLICY:

It is Department policy that:

- DOH shall ensure that it provides notice to all individual(s) affected by a security breach immediately following discovery or notification of breach.
- Any and all instances of a security breach shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective January 1, 2007.

I. **Ensure that personal information records are identified, minimized and properly secured.**

- A. **Inventory records.** Each DOH program shall identify and create an inventory of the records that it maintains or are maintained on its behalf that include personal information. The inventory should include the types of personal information maintained, the location of the record (whether on-site or off) and the employees or any third parties who are authorized to access the records. The inventory does not need to list each record or document, but should describe the types of records maintained and the respective purposes for which the personal information is permitted to be used and/or disclosed.
- B. **Minimize and eliminate.** Each DOH program shall review their data collection policies to determine whether they can minimize or eliminate the collection of personal information. Programs may consider collecting such information in redacted format (e.g., the last four digits of the Social Security numbers). In addition, programs shall consider whether existing records containing personal information are no longer needed. If not, they should be destroyed pursuant to DOH's Destruction of Personal Information Records policy.
- C. **Ensure security of information.** Each DOH program shall have written procedures that ensure the security of any records that contain personal information, whether maintained by the program or by third parties. Such procedures may require particular handling and storage techniques, including confidentiality agreements with third parties, and may limit access to the information to appropriate employees. Procedures should address, among other things, how and where such records are secured, who has access and how access is monitored (refer to the DOH intranet site for recommended security guidelines).

II. **Notification of security breaches.**

- A. DOH collects personal information for specific government purposes. Therefore, DOH shall provide notice that there has been a security breach to individual(s) affected by a security breach following discovery or notification of breach. The disclosure notification shall:
 - 1. Be made without unreasonable delay, with the exception of law enforcement requests pursuant to subsection II.c;
 - 2. Be consistent with any measures necessary to:
 - a. Determine sufficient contact information;
 - b. Determine the scope of the breach; and
 - c. Restore the reasonable integrity, security and confidentiality of the data system.

- B. Notification of owner or licensee of personal information affected by a security breach. DOH maintains or possesses records or data containing personal information of residents of Hawaii. Therefore, DOH shall notify any owner or licensee of personal information involving any security breach that there has been a security breach immediately following the discovery or notification of breach, with the exception of law enforcement requests, pursuant to subsection II.c.
- C. Law enforcement requests. DOH shall notify the individual(s) of a security breach, consistent with the legitimate needs of law enforcement as provided as follows:
1. The notice required by this section shall be delayed if a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such a request is made in writing, or DOH documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation.
 2. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to DOH its determination that notice will no longer impede the investigation or jeopardize national security.

III. Description of the disclosure notice.

- A. The notice shall be clear and conspicuous.
- B. The notice shall include a description of the following:
1. Incident in general terms;
 2. Type of personal information that was subject to the unauthorized access and acquisition;
 3. General steps taken by DOH to protect the personal information from further unauthorized access;
 4. Telephone number that the individual(s) may call for further information and assistance, if one exists; and
 5. Advice that directs the individual(s) to remain vigilant by reviewing account statements and monitoring free credit reports.

IV. Provision of the notice.

The notice to affected individual(s) may be provided by one of the following methods:

- A. Written notice to the last available address DOH has on record;
- B. Electronic mail notice, for those individual(s) for whom DOH has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. Section 7001;

- C. Telephonic notice provided that contact is made directly with the affected individual(s);
- D. Substitute notice, if DOH demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of subject individuals to be notified exceeds two hundred thousand or if DOH does not have sufficient contact information or consent as described above, for only those affected individuals without sufficient contact information or consent, or if the DOH is unable to identify particular affected individuals, for only those unidentifiable affected individuals. Substitute notice shall consist of all the following:
 - 1. Electronic mail notice when DOH has an electronic mail address for the subject persons;
 - 2. Conspicuous posting of the notice on the DOH website; and
 - 3. Notification to major statewide media.

V. Any waiver of the provisions of sections I-IV of this policy is contrary to public policy and is void and unenforceable.

VI. Reporting requirements.

Any and all instances of a security breach defined in this policy shall be immediately reported as outlined below.

- A. DOH program workforce member's responsibilities include, but are not limited to:
 - 1. Notifying his/her respective Office/Branch/Division Chief immediately after he/she becomes aware that a security breach may have occurred;
 - 2. Immediately documenting all relevant facts and circumstances of the security breach or potential security breach and submitting all documentation to his/her Office/Branch/Division Chief.
- B. Office/Branch/Division Chief's responsibilities include, but are not limited to:
 - 1. Receiving the initial report from a workforce member(s) or others of a security breach (alleged or confirmed) from his/her program's workforce members or others;
 - 2. Collecting and documenting relevant facts and circumstances of the reported security breach within two (2) working days. In addition, the chief shall complete a "Personal information security incident report form" (refer to the DOH intranet site for the standardized form);
 - 3. Immediately contacting and forwarding all relevant facts and circumstances (including the "Personal information security incident report form") regarding any security breach to his/her supervising Deputy Director and the DOH HIPAA Office;
 - 4. Being knowledgeable and familiar with this policy and the requirements and definitions;

5. Ensuring that his/her program's workforce member(s) are familiar with DOH security breach notification policies and that they understand the definition of "security breach" and "personal information" as defined therein.
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the security breach.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of a security breach (alleged or confirmed) from his/her Office/Branch/Division Chief;
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a security breach (alleged or confirmed);
3. Evaluating, assessing and determining if the initial incident/breach is defined as a security breach that is reasonably likely to or will actually result in illegal use of personal information and creates a risk of harm to the individual;
 - a. Evaluating and determining the appropriate response to the reported incident/breach which includes but is not limited to immediately contacting the Director and forwarding the relevant facts and circumstances regarding incident/breach to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's office of any security breaches. Such notice should be given to the Chief of Staff, the policy office and the communications office;
2. Initiating the notification process requirement for affected individual(s) of a security breach as defined in sections II-IV of this policy.
3. Reviewing and revising, if necessary, the written report to the legislature as provided by the Off/Branch/Division Chief. Assuming responsibility for the submittal of the required written report to the legislature regarding a security breach within 20 days of discovery as defined in section VII below.

VII. Legislative reporting requirements.

- A. The DOH shall submit a written report to the legislature within twenty days of discovery of a security breach. The report shall include, but is not limited to the following:
1. Detailed information relating to the nature of the breach;
 2. The number of individuals affected by the breach;
 3. A copy of the notice of security breach that was issued;

4. The number of individuals to whom the notice was sent;
5. Whether the notice was delayed due to law enforcement considerations;
6. Any procedures that have been implemented to prevent the breach from reoccurring.

B. In the event that a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

VIII. Corrective Action Plan. The involved DOH program shall submit a Corrective Action Plan addressing any security breach to the Director's Office and the DOH HIPAA Office within thirty days after the discovery of a security breach. The Corrective Action Plan shall include but is not limited to the following:

- A. The specific area(s) of improvement identified that could prevent a further security breach similar to the one that occurred;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent the type of breach from reoccurring;
- C. A timeline indicating when the program intends to have the procedure(s) and/or activities fully implemented;
- D. Specific measures that will describe how progress will be tracked and evaluated by the program.

IX. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervising chiefs immediately after they become aware of a security breach.

X. Implementation of policy.

- A. All DOH programs shall develop and implement procedures that comply with this policy by January 1, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy and implement procedures that comply with this policy by January 1, 2007.

XI. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor security incidents and breaches on an annual or as needed basis.
- B. The HIPAA Office shall evaluate and respond to the acceptability of the DOH program's Corrective Action Plan.

REFERENCES:

HRS § 487N

15 U.S.C. § 7001

September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies.

RELATED POLICIES:

DOH Policy P02.05 – Privacy Complaints

DOH Policy P04.02 – Privacy Incidents

DOH Policy P27.01 – Destruction of Personal Records

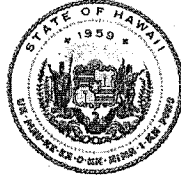
ATTACHMENTS:

Personal Information Security Incident Report Form

APPROVED:



Chiyome Leinaala Fukino, M.D., Director of Health



Policy Number: P27.01
Version Number: 2

Initial Approved Date: December 15, 2006
Last Modification Date: MM/DD/YY

TO:

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM:

Director of Health

SUBJECT:

Destruction of Personal Information Records

SCOPE:

Department of Health – All Programs

PURPOSE:

To decrease the risks of identity theft by establishing policies and guidelines relating to the adequate destruction or proper disposal of the Department of Health ("DOH") records containing personal information and to comply with the requirements of Hawaii Revised Statutes ("HRS") Chapter 487R.

POLICY:

It is Department policy that:

- DOH shall ensure that records containing personal information are properly destroyed before they are discarded, irrespective of whether the records are maintained by the program or by third parties.
- Any and all instances of a material occurrence of unauthorized access to personal information records in connection with or after its disposal shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective January 1, 2007.

I. Destruction of personal information records.

- A. DOH collects and maintains records containing personal information of Hawai'i residents. Therefore, it shall take reasonable measures to protect against the unauthorized access to or use of personal information it maintains in connection with or after its disposal.
- B. Paper records. Reasonable measures for destroying paper records containing personal information shall include:
1. Implementing and monitoring compliance with policies and procedures that requires the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practically read or reconstructed.
 2. It is DOH's policy that paper records containing personal information shall comply with DAGS' record destruction policy (Refer to: DAGS. Disposal of Government Records, April 12, 2005-revised August 1, 2006).
 - a. Pursuant to DAGS' record destruction policy, proper destruction includes but is not limited to shredding of paper documents using shredders.
 - b. It is DOH's policy that shredders must meet at least DIN 32757 Security Level 3. DIN (Deutsches Institut fur Normung) or the German Institute for Standardization developed security standards for paper shredders.
 - i. Security Level 3 is designed for shredding confidential paper documents and personal data. DIN 32757 Security Level 3 certified shredders will shred paper to 1/16-inch (strip cut); 1/8-inch x 1 1/8 inch (cross cut).
- C. Electronic records. Reasonable measures for destroying electronic records containing personal information shall include:
1. Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practically be read or reconstructed.
 2. It is the Department's policy that electronic records containing personal information shall comply with DAGS' record destruction policy (Refer to: DAGS. Disposal of Government Records, April 12, 2005-revised August 1, 2006.) In addition, programs shall consult with the DOH Health Information Systems Office regarding acceptable standards for properly sanitizing and disposing of electronic records and equipment.
- D. Contracting with a disposal business and due diligence. DOH may satisfy its obligation hereunder by exercising due diligence and entering into a written contract with, and thereafter monitoring compliance by, another party engaged in the business of record destruction to destroy personal information in a manner consistent with this section. Due diligence should at minimum include one or more of the following:
1. Reviewing an independent audit of the disposal business's operations for compliance with these policies, with HRS Chapter 487R;

2. Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party, such as the National Association for Information Destruction (NAID) (www.naidonline.org), with a reputation for high standards of review; or
3. Reviewing and evaluating the disposal business' information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal business.

E. Third parties maintaining personal information records on behalf of DOH.

1. Third parties that maintain records that contain personal information on behalf of DOH programs must follow DOH's policy for destroying records. Programs are responsible for ensuring that any such third parties are contractually bound to follow this policy and the requirements of HRS Chapter 487R.

II. Reporting requirements.

Any and all instances of a material occurrence of unauthorized access to personal information records in connection with or after its disposal shall be immediately reported as outlined below.

A. DOH workforce member's responsibilities include, but are not limited to:

1. Notifying his/her respective Office/Branch/Division Chiefs immediately after he/she becomes aware of any material occurrence of unauthorized access to records containing personal information in connection with or after its disposal.
2. Immediately documenting all relevant facts and circumstances of the material occurrence of unauthorized access to records containing personal information in connection with or after its disposal.

B. Office/Branch/Division Chief's responsibilities include, but are not limited to:

1. Receiving the initial report from workforce member(s) or others of any material occurrence of unauthorized access to personal information records in connection with or after its disposal;
2. Collecting and documenting relevant facts and circumstances of the reported material occurrence of unauthorized access to personal information records in connection with or after its disposal within two (2) business days. In addition, the chief shall complete a "personal information disposal incident report form" (refer to the DOH intranet site to locate the standardized form);
3. Immediately contacting and forwarding the relevant facts and circumstances (including the "personal information disposal incident report form") regarding any material occurrence of unauthorized access to personal information records in connection with or after its disposal to his/her supervising Deputy Director and the HIPAA Office;

4. Being knowledgeable and familiar with this policy and the requirements and definitions in HRS Chapter 487R;
5. Ensuring that his/her program's workforce members are familiar with and trained in DOH's disposal and reporting policies and that they understand the definitions of "personal information", "records", and "disposal" as defined therein.
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the security breach.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of any material occurrence of unauthorized access to personal information records in connection with or after its disposal from his/her Office/Branch/Division Chief.
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Privacy Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a material occurrence of unauthorized access to personal information records in connection with or after its disposal.
3. Evaluating, assessing and determining if the initial incident/occurrence is defined as a material occurrence of unauthorized access to personal information records in connection with or after its disposal.
4. Evaluating and determining the appropriate response to the reported incident/occurrence which includes immediately contacting the Director and forwarding the relevant facts and circumstances regarding any material occurrence of unauthorized access to personal information records in connection with or after its disposal to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's Office of any material occurrence of unauthorized access to personal information records in connection with or after its disposal. Such notice should be given to the Chief of Staff, the Policy Office and the Communications Office.
2. Reviewing and revising, if necessary the written report to the legislature by the Office/Branch/Division Chief. Assuming responsibility for the submittal of the required written report to the legislature regarding the unauthorized access within 20 days of discovery in section III below.

III. Legislative reporting requirements.

- A. DOH shall submit a written report to the legislature within twenty (20) days of discovery of a material occurrence of unauthorized access to personal information in connection with or after its disposal. The report shall include, but is not limited to the following:
 - 1. Detailed information relating to the nature of the incident;
 - 2. The number of individuals affected by the incident; and
 - 3. Any procedures that have been implemented to prevent the incident from reoccurring.
- B. In the event that a law enforcement agency informs DOH that the report may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

IV. Corrective Action Plan. The involved DOH program shall submit a Corrective Action Plan addressing any material occurrence of unauthorized access to personal information records in connection with or after its disposal to the Director's office and the DOH HIPAA office within thirty days after the discovery of a material occurrence. The Corrective Action Plan shall include but is not limited to the following:

- A. The specific area(s) of improvement identified that could prevent further material occurrences;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent similar incidents from reoccurring;
- C. A timeline indicating when the program intends to have the above procedure(s) and/or activities fully implemented; and
- D. Specific measures that describe how progress will be tracked and evaluated by the program.

V. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervisor immediately after they become aware that:
 - 1. Records containing personal information have not been destroyed in accordance with this policy; and
 - 2. There has been unauthorized access to personal information disposed of, by or on behalf of their respective programs.

VI. Implementation of policy.

- A. All DOH programs shall develop and implement records disposal and reporting procedures that comply with this policy by January 1, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy by January 1, 2007.

VII. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor material occurrences of unauthorized access to personal information records in connection with disposal on an annual or as needed basis.
- B. The HIPAA Office shall evaluate and respond to the acceptability of the Corrective Action Plan.

REFERENCES:

HRS § 487R

September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies

RELATED POLICIES:

DOH Policy P02.05 – Privacy Complaints

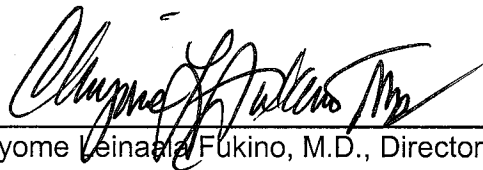
DOH Policy P04.02 – Privacy Incidents

DOH Policy P26.01 – Notification of Security Breach

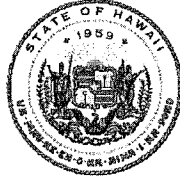
ATTACHMENTS:

Personal Information Disposal Incident Reporting Form

APPROVED: _____



Chiyome Veinana Fukino, M.D., Director of Health



Policy 28.01
Version Number: 2

Initial Approved Date: February 26, 2007
Last Modification Date: March 17, 2008

TO:

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM:

Director of Health

SUBJECT:

Social Security Number Protection

SCOPE:

Department of Health – All Programs

PURPOSE:

To decrease the risks of identity theft by establishing Department of Health (“DOH”) policies and guidelines relating to the protection of records containing social security numbers from unauthorized access and to comply with Hawaii Revised Statutes (“HRS”) Chapter 487J.

POLICY:

It is Department policy that:

- DOH shall ensure that reasonable procedural safeguards are implemented to protect against unauthorized access to program records containing social security numbers.
- Any and all instances of unauthorized access to records containing social security numbers shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective March 5, 2007.

I. Protection of social security numbers.

A. Identify records containing social security numbers.

1. Each DOH program shall create an inventory of records that contain social security numbers within thirty (30) days of the effective date of this policy.
2. Each DOH program shall conduct an annual update of this inventory.
3. This inventory shall include the numbers, types, locations, and purposes of these records along with a list of those workforce members who are authorized to access the records.

B. Minimize, eliminate, and redact.

1. DOH programs shall determine whether they can minimize or eliminate the collection of social security numbers.
2. Whenever possible, DOH programs shall maintain social security numbers in redacted form (last four digits).
3. DOH programs shall determine which existing records are no longer needed. These records should be properly destroyed to prevent unauthorized access to individuals' social security numbers (refer to DOH Policy 27.01 Destruction of Personal Information Records).

C. Implement safeguards.

1. DOH programs shall implement reasonable safeguards to prevent unauthorized access to social security numbers which are collected and maintained. (Refer to DOH Intranet "Guidelines for Protecting Confidential Information").

D. Activities related to social security numbers that are NOT permitted.

1. Intentionally communicating or otherwise making available to the general public an individual's entire social security number.
2. Intentionally printing or imbedding an individual's entire social security number on any card required for the individual to access services provided by a DOH program.
3. Requiring an individual to transmit the individual's entire social security number over the internet, unless the connection is secure or the social security number is encrypted.
4. Requiring an individual to use the individual's entire social security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website.

5. Printing an individual's entire social security number on any materials that are mailed to the individual, unless the materials are employer-to-employee communications, or where specifically requested by the individual.

E. Activities related to social security numbers that are permitted:

1. The inclusion of a social security number in documents that are mailed and:

- a. Are specifically requested by the individual identified by the social security number;
- b. Required by state or federal law to be on the document to be mailed;
- c. Required as part of an application or enrollment process;
- d. Used to establish, amend, or terminate an account, contract, or policy; or
- e. Used to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b).

(1) Note: A social security number that is permitted to be mailed may **NOT** be:

- ◆ Printed, in whole or in part, on a postcard or other mailer not requiring an envelope; nor
 - ◆ Visible on the envelope or without the envelope having been opened.
2. The opening of an account or the provision of or payment for a product or service authorized by an individual.
 3. The collection, use, or release of a social security number to:
 - a. Investigate or prevent fraud;
 - b. Conduct background checks;
 - c. Conduct social or scientific research;
 - d. Collect a debt;
 - e. Obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 to 1681x, as amended;
 - f. Undertake a permissible purpose enumerated under the federal Gramm Leach Bliley Act, 15 U.S.C. §§ 6801 to 6809, as amended;
 - g. Locate an individual who is missing or due a benefit, such as a pension, insurance, or unclaimed property benefit; or

- h. Locate a lost relative.
- 4. Acting pursuant to a court order, warrant, subpoena, or when otherwise required by law.
- 5. Providing the social security number to a federal, state, or local government entity including a law enforcement agency or court, or their agents or assigns.
- 6. The collection, use, or release of a social security number in the course of administering a claim, benefit, or procedure relating to an individual's employment, including:
 - a. An individual's termination from employment;
 - b. Retirement from employment;
 - c. Injuries suffered during the course of employment;
 - d. Other related claims, benefits, or procedures.
- 7. The collection, use, or release of a social security number as required by state or federal law.
- 8. The sharing of the social security number by business affiliates.
- 9. The use of a social security number for internal verification or administrative purposes.
- 10. The use or sharing of a social security number that has been redacted.
- 11. Documents or records that are recorded or required to be open to the public pursuant to the constitution or laws of the State or court rule or order.

II. Reporting requirements.

Any and all instances of a material occurrence of unauthorized access to records containing social security numbers shall be immediately reported as outlined below.

- A. DOH program workforce member's responsibilities include, but are not limited to:
 - 1. Notifying his/her respective Office/Branch/Division Chief immediately after he/she becomes aware of any material occurrence of unauthorized access to records containing social security numbers may have occurred.
 - 2. Immediately documenting all relevant facts and circumstances of the material occurrence of unauthorized access and submitting all documentation to his/her Office/Branch/Division Chief.

B. Office/Branch/Division Chief's responsibilities include, but are not limited to:

1. Receiving the initial report from a workforce member(s) or others of any material occurrence of unauthorized access to records containing social security numbers (alleged or confirmed) from his/her program's workforce members or others;
2. Collecting and documenting relevant facts and circumstances of the reported material occurrence within two (2) working days. In addition, the Chief shall complete a "Personal Information Security Incident Report Form" (refer to the DOH Intranet site for the standardized form);
3. Immediately contacting and forwarding the relevant facts and circumstances (including the "Personal Information Security Incident Report Form") regarding any material occurrence to his/her supervising Deputy Director and the DOH HIPAA Office;
4. Being knowledgeable and familiar with this policy and the requirements and definitions in HRS Chapter 487J;
5. Ensuring that his/her program's workforce member(s) are familiar with and trained in DOH's reporting policies;
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the disclosure.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of any material occurrence of unauthorized access to records containing social security numbers from his/her Office/Branch/Division Chief;
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a material occurrence of unauthorized access to records containing social security numbers.
3. Evaluating, assessing and determining if the incident is defined as a material occurrence of unauthorized access to records containing social security numbers; and if it is reasonably likely to or will actually result in illegal use of an individual's social security number and creates a risk of harm to the individual (refer to "security breach" DOH Policy P26.01 Notification of Security Breaches);
4. Evaluating and determining the appropriate response to the reported incident/disclosure which includes but is not limited to immediately contacting the Director and forwarding the relevant facts and circumstances regarding any material occurrence of unauthorized access to records containing social security numbers to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's office of a material occurrence of unauthorized access to records containing social security numbers. Such notice should be given to the Chief of Staff, the Policy Office and the Communications Office;
2. Reviewing and revising, if necessary, the written report to the legislature as provided by the Office/Branch/Division Chief.
3. Assuming responsibility for the submittal of the required written report to the legislature regarding the unauthorized access within twenty (20) days of discovery as defined in section III below.

III. Legislative reporting requirements.

- A. The DOH shall submit a written report to the legislature within twenty (20) days of discovery of a material occurrence of unauthorized access to records containing social security numbers. The report shall include, but is not limited to the following:
 1. Detailed information relating to the nature of the incident;
 2. The number of individuals affected by the incident; and
 3. Any procedures that have been implemented to prevent the incident from reoccurring.
- B. In the event that a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty (20) days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

IV. Corrective Action Plan.

The involved DOH program shall submit a Corrective Action Plan addressing any material occurrence of unauthorized access to records containing social security numbers to the Director's Office and the DOH HIPAA Office within thirty (30) days after the discovery of a material occurrence. The Corrective Action Plan shall include but is not limited to the following:

- A. The specific area(s) of improvement identified that could prevent any future material occurrences;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent similar incidents from reoccurring;
- C. A timeline indicating when the program intends to have the procedure(s) and/or activities fully implemented; and
- D. Specific measures that will describe how progress will be tracked and evaluated by the program.

V. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervising chiefs immediately after they become aware of an occurrence of unauthorized access to records containing social security numbers.

VI. Implementation of Policy.

- A. All DOH programs shall develop and implement procedures that comply with this policy by April 2, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy and implement procedures that comply with this policy by April 2, 2007.

VII. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor material occurrences of unauthorized access to records containing social security numbers on an annual or as needed basis.
- B. The HIPAA Office shall evaluate and respond to the acceptability of the Corrective Action Plan.

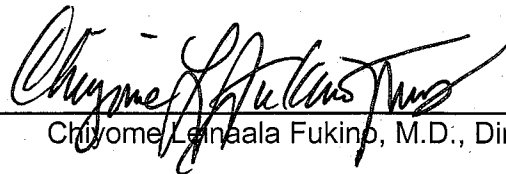
REFERENCES:

HRS § 487J

15 U.S.C. §1681(b)

September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies.

APPROVED: _____



Chiyome Linaala Fukino, M.D., Director of Health