HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Corporate HR Office	Policy No.: **HR 0010**
		Revision No.: 1
Policies and Procedures	Issued by: VP/Dir of Human Resources	Effective Date: April 15, 2008
Subject: ***Protection of Personnel Information Program***	Approved by: Hawaii Health Systems Corp. By: Thomas M. Driskill, Jr. President & CEO	Supersedes Policy: December 19, 2007
		Page: 1 of 20

I. PURPOSE: To establish procedures related to personnel information to comply with various State laws (HRS Chapter 487J - Social Security Number Protection, Chapter 487N - Security Breach of Personal Information, and Chapter 487R - Destruction of Personal Information Records) which were enacted to protect individuals from identity theft.

II. BACKGROUND: Hawaii Health Systems Corporation (HHSC) has viewed, and continues to view, some of the personnel information collected and maintained on employees and applicants as confidential information. (At the same time, HHSC acknowledges that some personnel information must be disclosed under the State's Uniform Information Practices Act.) The rise in identity theft nationwide and the enactment of State laws to address identity theft (HRS Chapters 487J, 487N, and 487R) have prompted HHSC to formalize its practices related to the protection of personnel information. This document provides procedures and guidelines for the handling of personnel information and details actions that must be taken in the event of a breach of such information.

III. SCOPE: Information collected and maintained in hard copy forms and/or electronic form by authorized employees of the Human Resources Offices.

IV. POLICY:

A. It is the policy of the Hawaii Health Systems Corporation to endeavor to secure applicant and employee personnel information from unauthorized disclosure, loss or theft.

B. The policy does NOT cover medical information or drug and alcohol testing information. Such information remains highly confidential and is covered by other laws, rules or policies. Breaches involving such information should be reported to the HHSC designee with overall responsibility for the particular program. If the information contains personal information (as defined in this policy); it may be subject to the notification requirements under the law.

V. DEFINITIONS:

A. "Disposal" defined in the law and means the discarding or abandonment of records containing personal information or the sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of

personal information, or other non-paper equipment for non-paper storage of information.

B. "Encryption" defined in the law and means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

C. "Personal information" defined in the law and means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social Security Number;
2. Driver's Licenses Number or Hawaii identification card number
3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

D. "Personnel information" means all individually identifiable information maintained on an employee for employment related purposes and which is under the jurisdiction of the Hawaii Health Systems Corporation—whether or not such information is also considered to be "personal information." This includes, but is not limited to, an employee's name, social security number, home address, birthdate, and salary.

E. "Records" defined in the law and means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

F. "Redacted" defined in the law and means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

G. "Security Breach" defined in the law and means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

H. "Information Breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personnel information where illegal use of the personnel information has occurred, or is reasonably likely to occur and that creates a risk of harm to person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personnel information along with the confidential process or key constitutes a

security breach. Good faith acquisition of personnel information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personnel information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

The definitions above which are defined in the law shall be considered amended whenever the definitions in the law are amended.

VI. RESPONSIBILITIES

A. The Vice President and Director of Human Resources (VP/DHR)

The VP/DHR shall be responsible for the following:

1. Designating a lead position to be responsible for the protection of personnel information program—.
   a. The designated position is: Personnel Program Officer - Classification
   b. The alternate is: Personnel Program Officer - Employment
2. Promulgating and maintaining procedures and guidelines intended to secure personnel information and comply with the laws related to the protection of personal information—including social security numbers.
3. Coordinating regional efforts to comply with the law as it relates to personnel information—including answering questions related to the law.
4. Auditing (as deemed necessary by the VP/Director of Human Resources) regional compliance with the procedures and laws.
5. Ensuring proper notification is provided to any employee affected by a breach in security or information.

B. HHSC's Information Technology Department (ITD)

The Information Technology Department shall be responsible for the following:

1. Ensuring that appropriate electronic data security programs and policies are established.
2. Ensuring that a Corporate Information Security Officer (CISO) position is responsible for Information Technology Security for the HHSC.
3. Ensuring that any requests to the ITD for personnel data on electronic media or printed hard copy are authorized in writing by the VP/DHR for programs indicated by HR (i.e., Lawson).
4. Ensuring that any information technology security incidents are reported and investigated by the CISO. Any HR related incident shall be reported to the VP/DHR and/or designee.

C. Regional Human Resources Directors (RHRD)

The RHRD shall be responsible for the following:

1. Coordinating the protection of applicant and employee personnel information collected and maintained for the respective region.

2. Authorizing and maintaining a list of employees who are authorized to handle and view personnel information for the respective region.
3. Ensuring that the procedures to secure personnel information and to comply with the laws are followed which includes monitoring compliance with the procedures on the protection and proper disposal of the materials that contain personnel information.
4. Ensuring that HHSC Corporate Office and other identified departments and agencies are promptly notified of a breach. Notifying the CISO for any breach of IT related issues.
5. Cooperating with the Corporate HR Office in its efforts to ensure compliance with the law as it relates to personnel information—including cooperating with any audits conducted by HHSC Corporate Office.

D. Employees Who are Authorized to Handle and View Personnel Information

Employees who are authorized to handle or view personnel information are responsible for the following:

1. Treating any personnel information the employee handles or becomes aware of as confidential (unless the information is clearly covered by laws deeming the information to be public information).

    a. An employee may become aware of information through various means, including, but not limited to, by hearing conversations in the workplace, seeing information on other workers' computer screens, etc. Whether an employee becomes aware of such personnel information through the course of his/her work, or by some other means, the requirements regarding confidential treatment of the information apply.

2. Disclosing personnel information only when authorized to do so and only to those who are authorized to receive the information. Unauthorized communication is strictly prohibited.

    a. Authorized disclosure may be via a written and signed request from an employee to disclose his/her records. Such requests should be reviewed by the Regional Human Resources Director and may be reviewed by the Corporate Counsel and the disclosure should only be for the records as authorized.

    b. Authorized disclosure may also be by normal processing procedures. (Even if the forms contain personal information, no other specific authorization is required. Facility HR Office must ensure that the transmittal is handled in a manner that protects the confidentiality of the information—hand carrying the documents or placing them in a sealed envelope marked "confidential." This shall include procedures such as processing Employee Transactions Report (ETR), Employee-Union Trust Fund [EUTF], and payroll electronic files.)

c. Authorized disclosure may also be made where a collective bargaining agreement requires the disclosure. However, the VP/DHR and the RHRD shall be consulted prior to the disclosure.

d. Authorized disclosure may also be necessary to respond to a subpoena or court order for personnel information. The RHRD shall be consulted before such a disclosure is made. If need be, the RHRD may consult with Legal Counsel before proceeding.

3. All employees who are authorized to handle and those who work with, personnel information shall be on alert for possible information breaches. If any are detected, the individual is to immediately notify the RHRD to ensure that the precautions are taken to secure the information and to ensure that the breach is handled in accordance with required procedures. After notifying the RHRD, the employee must treat information related to the breach as confidential. The reason for this is that the disclosure of the breach before assessments are made, and before appropriate actions are taken, by HHSC and/or law enforcement may result in the additional loss of information or may impede the investigation of the breach.

   Appropriate action, which may include disciplinary action, may be taken if an employee fails to properly protect personnel information or to otherwise comply with this program. The disciplinary action will be in accordance with the respective collective bargaining agreements and the HHSC Human Resources and Civil Service System Rules, as applicable.

VII. PROTECTION OF INFORMATION — GUIDELINES

It is recognized that one of the best ways to protect personal information is NOT to collect and/or provide the information unless it is required by law or otherwise necessary. Accordingly, HHSC Corporate Human Resources Office and the regional Human Resources Offices shall periodically review their personnel practices which require the collection of personal information and shall determine whether or not the collection of such information may be stopped.

A. Protection of Paper Records

1. Personnel records that contain personal information shall be retained in a secure location with limited access.
   a. Personnel folders that are not being actively worked on should be stored in locked file cabinets.
      i. Personnel folders for employees who have separated from service shall be placed, by HHSC and/or its Regional HR Offices, in the States' archive facilities which has restricted access.
   b. Ideally, individual personnel records that contain personal information that are not being actively worked on should be stored in locked file cabinets or desks.
      i. This includes all personnel related forms that contain social security numbers, such as personnel action forms (Lawson ETR forms), Employees' Retirement System forms, and Employer-Union Trust forms.

ii. Individual personnel records that do not contain personal information, as defined, may still contain confidential and sensitive information—such as home addresses—which must be protected from disclosure in the same manner.

c. Personnel records that are being actively worked on should be protected by the individual working on the records. If the individual leaves his/her desk, the record should be secured.
   i. The record will be considered secured if it is locked in the individual's desk, locked in a file cabinet with limited access or locked in an individual office.
   ii. Individuals who work in offices with restricted access where all employees in the office handle confidential personnel information may secure the record by covering the record or turning it over.

d. The Human Resources Offices who do not have adequate locking storage devices to secure work in progress should include the acquisition of such devices in their long term plan. It is assumed that facilities have already obtained adequate locking files to hold their personnel folders.

B. Protection of Electronic Records

Personnel Records in electronic form must be afforded the same or higher level protection as paper records.

1. Adherence to the policies and procedures established by HHSC's Information Technology Department for data security, computer system back up, and the use of internet and email is required by all individuals who handle personnel information.
2. Employees must take precautions to secure the computers on which they view personnel information. This includes, but is not limited to, requiring a password to log on to the computer and having the screen saver come on after a short period of inactivity. Accessing the computer after the screen saver is activated requires the typing in of the password
   a. Employees must take special precautions with laptop computers and must NOT store personnel information that contains personal information on the laptop computers.
3. Employees may not place or store personnel information on removable devices and media such as flash drives, CDs, DVDs, tapes, or diskettes unless authorized according to HHSC's normal processing procedures **and/or** the employee must ensure that the information has been encrypted (NOT just password protected).
   a. At no time should employees place large amounts of personnel information onto these devices—such as placing the names, addresses and phone numbers of all employees in the facility on a diskette.
      i. An exception may be made by the Regional Human Resources Director if the information is required for the employee's job and must be in a removable form. The employee having custody of the data must secure the removable device and the data. HHSC plans to implement programs to give the capabilities for this type of data encryption.

4. Employees must not place personnel information in electronic folders on file servers that are accessible to other employees who are not authorized to access this personnel information.
5. Employees must take precautions when faxing or emailing personnel information, particularly if it contains personal information. In general personal information should not be sent by fax or email, unless document is sent to a secured location accessible by authorized personnel only. Entire Social Security numbers must not be sent by fax or email, unless it's required by an authorized agency conducting business with HHSC. The last four digits of a social security number should be used if the authorized agency does not require the complete social security number.

C. Special Precautions for Social Security Numbers

1. The law (HRS Chapter 487J) provides special protection for Social Security Numbers. Although the law provides a specific exclusion for 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, HHSC and it's facilities continues to view the social security number as highly confidential information which is to be afforded proper protection. In addition, some uses and disclosure of social security numbers fall outside of the strict employment areas. Accordingly, Regional Human Resources Directors must review and comply with the specific requirements under the law when social security numbers are collected, used or disclosed.
2. The following are recommended practices related to the use of social security numbers.
   a. Social security numbers should not be used unless there is a business requirement for their use. If the social security number is required, care must be taken to ensure that the information is protected. For example, when transmitting Employees' Retirement System forms containing social security numbers it is recommended that a cover sheet also be sent listing all the forms being transmitted and requesting confirmation of receipt. When transmitting electronic files containing social security numbers, the file must be encrypted unless an exception has been made in writing by the VP/DHR. If an exception has been made, the file must, at a minimum, be password protected.
   b. If a social security number must be used, whenever possible, only the last four digits should be used.
   c. Social security numbers are not to be printed or imbedded on any employee identification card or any other card required for access.
   d. Employees will not be required to transmit their entire social security number over the internet or required to use their entire social security number for access to an internet website (unless the requirements set by law for exception to these standards are met).
   e. Entire Social Security numbers should generally not be printed on materials mailed to the individual. However, if the information must be printed (and the law permits the printing of the entire social security number) the authorized personnel must take appropriate precautions when mailing the materials containing the social security numbers. For

example, the social security number must not be visible—the document must be in a sealed envelope and the social security number cannot be visible on the envelope or without the envelope having been opened.

VIII. NOTIFICATION OF BREACH

Under HRS Chapter 487N, we are required to notify affected individuals when we discover or are notified of a security breach. The VP/DHR may also require notification to affected individuals of information breaches that involve personnel information that does not contain personal information (such as breaches involving an employee's name, address and birthdate).

A. Notification in HHSC

When an information breach is first identified, it is important to determine the scope of the breach, to secure the information and to determine if any delays in notification are necessary. Since disclosure of a breach may result in additional loss of information or may impede a criminal investigation, it is essential that the number of individuals initially notified be kept to a minimum. The following individuals must be notified of a breach (if any of the individuals below is suspected of being involved in the breach, notify their alternate or higher level supervisor in place of the designated individual):

1. Regional Human Resources Director. The RHRD serves as the point of contact for breaches on employee personnel and personal information being stored and maintained by that regional Human Resources Office. The RHRD shall notify the VP/DHR and the VP/IT.
2. All breaches must be reported immediately to the designated HR & IT positions. Each region shall have positions responsible for the protection of employee designated personnel information and they must be notified of ALL personnel information breaches pertaining to their respective regions. The HHSC Director of End User Support, Corporate Information Security Officer must be notified of all breaches involving personnel information on electronic files, devices or media—including personnel information stored on laptops. The notification must be made even if the data is encrypted. The HHSC Director of End User Support, Corporate Information Security Officer serves as the point of contact for all breaches involving the loss or theft of information from HHSC's main computer system. The HHSC Director of End User Support, Corporate Information Security Officer may also request to serve as the point of contact for other incidents of the loss of electronic data.
3. General Counsel. The VP and General Counsel and the assistant General Counsel for Human Resources matters must be notified of all breaches involving personnel information.
4. Police Department (PD). The PD must be contacted whenever illegal actions are suspected—the theft of computer equipment, a lock on a file is broken, personnel folders are stolen, etc. A copy of the police report must be

obtained and retained in the file. PD may request a delay in notification (see subsection B. below).

B. Notification Delays

Notification to affected individuals must be made promptly so that these individuals can take action to protect their identity. However, there are legitimate reasons, permitted by law, to delay the notification.

1. Notification Delays Requested by a Law Enforcement Agency

A law enforcement agency may request that notification to affected individuals be delayed as disclosure would impede the investigation or jeopardize national security. Documentation of this request is required. The preferred method of documentation is a written request, signed by a representative of the law enforcement agency making the request. If properly documented, a verbal request is acceptable under the law. However, the department should attempt to obtain a written confirmation of the request. (See attached documentation forms for written and verbal requests.)

2. Pre-notification Activities

Although not deemed a delay under the law, the law acknowledges and provides for certain pre-notification activities. A facility, upon being notified of a breach, must engage in these activities to determine the scope of the breach, restore the integrity, security and confidentiality of the data system and determine the sufficiency of the contact information. These activities are essential to ensuring, to the extent possible, that all affected individuals are identified and notified, and to protect HHSC, its facilities, and individuals from further information loss.

C. Notification to Affected Individuals

1. Content of the Notice

The notice must be clear and conspicuous and must meet the requirements under the law. A sample notice is provided. It is essential that all elements be included. If the department elects not to follow the sample notice, the department must ensure that all elements required by law are followed.

2. How the Notice is Provided

The notice may be provided via one of the following methods:

a. Written Notice. A written notice sent to the individual's last known address on record with the facility or HHSC.

b. Notice via email. A notice via email is permitted. However, the individual must have agreed in advance to receive communications electronically and the notice must be provided in a manner consistent with the provisions set forth in 15 U.S.C. Section 7001 (see link below). If email is used to expedite the notification, HHSC requires that a written notice also be provided.

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+15USC7001

c. Telephonic notice. A notice via telephone call is permitted. However, the contact must be directly with the affected person. Leaving voicemail or other messages (other than to request a call back) is prohibited. If telephonic notice is used to expedite the notification, HHSC requires that a written notice also be provided.

d. Substitute notice.

i. Substitute notice is not the preferred method of providing the notice, however, if one of the following applies, a substitute notice may be provided:
- If the cost of providing the notice would exceed $100,000;
- If the affected class of subject persons to be notified exceeds 200,000, or;
- If the department is unable to identify all affected persons. However, the substitute notice may only be provided to those who are unidentified. All identified individuals must be notified by one of the methods above.

ii. The substitute notice must consist of all of the following:
- Electronic mail notice when the department has an email address for the subject persons;
- Conspicuous posting of the notice on the website of the facility or HHSC's website, or;
- Notification to major statewide media.

iii. Prior to using a substitute notice, the facility must consult with the VP/HR Director.

D. Notification to Regulating Agencies

1. Legislature

HHSC is required to provide a written report to the legislature within 20 days after the discovery of a security breach. If a law enforcement agency requests a delay in notification, the report to the legislature would also be delayed until 20 days after the law enforcement agency determined that the notice would no longer impede the investigation or jeopardize national security. A sample report is attached. If HHSC does not use the sample

report, HHSC must ensure that all the information required by law is included.

2. Other agencies
If more than 1,000 individuals must be notified of a security breach at one time (one incident), HHSC must send a written notification to the State of Hawaii's Office of Consumer Protection and to all consumer reporting agencies (Equifax, Experian, & TransUnion) that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p) (see link below). Sample letters to the Office of Consumer Protection and to the credit bureaus are attached.

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+15USC1681a

IX. DISPOSAL OF INFORMATION

Personnel information must not only be protected while being retained by a facility, but also must be protected by using proper disposal techniques when the paper or non-paper (such as electronic) document or files or media containing the information are no longer needed.

A. Paper Documents

All paper documents containing personnel information must be destroyed in such a manner that the information cannot practicably be read or reconstructed. The following methods, in addition to Dept. of Accounting & General Services' (DAGS) - General Records Schedule and disposal procedures, are considered acceptable:

1. Burning. A representative of the facility controlling the records must witnesses the documents being burned.
2. Pulverizing. A representative of the facility controlling the records must witness the pulverizing of the documents.
3. Shredding. If not doing the shredding, a representative of the facility controlling the records must witness the shredding of the documents.

B. Electronic Documents

All electronic documents, files or media (including hard drives, laptops, CDs, and other removable devices) containing personnel information must be destroyed or erased in such a manner that the information cannot practicably be read or reconstructed. Refer to HHSC Policy ITD 0023, Disposal/Reuse of Electronic Storage Media for acceptable methods of destruction.

C. Hiring a Contractor to Destroy the Records

The law permits government agencies to fulfill their disposal obligations by contracting with a company that is engaged in the business of records destruction.

Facilities electing to use such a company must ensure that all requirements of the law are met.

X. TRAINING AND CERTIFICATION OF RECEIPT OF MATERIALS

A. Corporate Human Resources and/or the Regional HR office shall offer training to employees who are authorized to handle confidential personnel information. This training shall be conducted in a similar fashion to the HIPAA and Corporate Compliance Training.

B. Corporate Human Resources and/or the Regional HR office shall offer refresher training, as deemed necessary, for employees who are authorized to handle personnel information.

C. Whether or not an employee who is authorized to handle confidential personnel information has completed the training, the employee must be provided with a copy of this policy.

D. Employees who have read and/or received a copy of the policy must acknowledge their understanding of the the basic confidentiality requirements by signing the Certificate of Understanding form. (Attached.)

Facility: ****

Department: _____

Protection of Personnel Information
Certificate of Understanding

I acknowledge that I have been provided an electronic, hard copy or have read completely the Protection of Personnel Information Program Document. I understand that if I have read the policy or received an electronic copy that I can request a hard copy of the document be given to me prior to my signing this certificate. I understand that the program covers not only the protection of the information, but also the proper methods of disposing of the information and the proper handling of suspected or detected breaches (unauthorized access/disclosure) of personnel information.

I understand that because I am authorized to handle certain personnel related documents, I am covered under the program and I am responsible for reviewing the materials and understanding my role in the program. I further understand that I am generally responsible for protecting any personnel information, and in particular personal information, that I may become aware of while performing my duties, while otherwise on HHSC and it's affiliates premises or in any other manner or from any other source connected with my job. I understand that I may become aware of personnel information in a number of ways including, but not limited to, my official handling of the information as part of my job duties, hearing conversations involving such information, or seeing such information on computer screens. I understand that the program and my responsibilities related to the protection of the information apply no matter how I became aware of the information.

I understand that if I suspect or detect a breach of the personnel information I must immediately contact _____ (or his/her successor or designee), the Regional Human Resources Director for personnel information protection for my facility. In addition, if I have any questions regarding the program or my role, I have been advised to contact my Regional Human Resources Director (or his/her successor or alternate).

_____ _____
Signature Date

_____
Printed Name

Protection of Personnel Information
Law Enforcement Request to Delay Notification

I, _____, a law enforcement officer with _____
Name (print or type) Law Enforcement Agency

request that _____, NOT provide notification to the affected
Agency Reporting the Breach

individuals of the breach/suspected breach reported on _____ regarding

_____
(Describe the Breach)

_____

at this time because doing so may impede a criminal investigation or jeopardize national security. I will notify the agency promptly when notifying the affected individuals will no longer impede the criminal investigation or jeopardize national security.

Signature: _____ Date: _____

Title: _____ Phone No.: _____

Original Date of Delay Request (if different from above): _____

For HHSC – Facility Use ONLY

Date advised that the notification to affected individuals will no longer impede the criminal investigation or jeopardize national security:

Name of Person Advising the Agency: _____

Name of Person Receiving the Advisory: _____

Advisory made in writing: ____ Yes _____ No

Date Notification Made to Affected Individuals: _____

****
Remarks (Include any notations of dates when follow-up calls were made to the law enforcement agency to see if the request to delay should be lifted):

Protection of Personnel Information
Law Enforcement Request to Delay Notification
Agency—Documentation of Request

Note: This is NOT the preferred method of documenting a request from law enforcement to delay the notification. It may, however, be used to document that a request to delay was NOT made or to temporarily document a verbal request. (However, the department should still make an effort to obtain written confirmation of the request.)

All the following information must be recorded contemporaneously (at the same time) the request is made by a representative of the law enforcement agency:

Date: _____ Time: _____ _____ A.M. _____ P.M.

Name of the Law Enforcement Officer Making the Request: _____

Title of the Law Enforcement Officer Making the Request: _____

Protection of Personnel Information
Notification to Affected Individuals
Breaches Involving **Personal Information**

*Note: The VP/Director of Human Resources may require that a similar notice be sent when there is a breach of **personnel** information that does NOT contain **personal** information.*

SECURITY BREACH—YOU MAY BE AT RISK FOR IDENTITY THEFT

Name
Address
City/State/Zip

Dear _____:

This is to notify you of an incident involving your personal information--**You should take action NOW to protect yourself from identity theft.**

_____ (*Department*) has (*been notified **or** discovered*) a security breach involving your personnel information. The incident (*describe the incident in general terms*). The information which (*has been **or** is suspected of being*) (*lost **or** stolen **or** acquired*) includes the following: (*list the type of information—SSN, etc.*).

To protect yourself, we recommend that you immediately place a fraud alert on your credit file and that you carefully monitor all your accounts (bank accounts, credit card accounts, etc.). The fraud alert will let creditors know they have to follow certain procedures (including contacting you) before opening new accounts in your name. The alert may be placed on your file by contacting any one of the three credit reporting agencies at the numbers listed below:

Equifax	Experian	Trans Union
1-800-525-6285	1-888-397-3742	1-800-680-7289

(*If the breach involved more than 1,000 individuals, include the following statement in the notice* ”The credit bureaus above have been alerted that a breach has occurred.”)

When talking with the credit reporting agencies, you should mention that you have been notified of a security breach involving your personal information. (It may be helpful to have this letter at hand when calling the credit agencies.) If you do not receive a confirmation that a fraud alert has been placed on your account from each of the above agencies, you should contact the agency and request that a confirmation be sent.

We also recommend obtaining a credit report from each of the three agencies above now and periodically (every three months for the first year at least) in the future (since you have placed a fraud alert on your account, the first report should be free; however, there may be a cost for future reports). **For your protection, we recommend that you ask that any report sent to you only list the last four digits of your social security number.** When you receive the reports, you should carefully review them to determine if there is any unusual activity—such as new accounts that you did not open, or inquiries from companies (like credit card companies) whose services (credit cards) you did not apply for. You should also check your personal information

to ensure that it is accurate—your home address is correct and has not changed, your social security number is correct, your employer information is correct, etc. If you need to make any corrections, or there is something you do not understand, contact the credit reporting agency immediately (a contact number should be listed on the report). When you obtain a credit report, you may also want to renew the fraud alert on your account.

If you notice any suspicious activity on your credit report or in any of your accounts, contact the Honolulu Police Department immediately (and if you are located outside of the City and County of Honolulu, your local police department) and file an identity theft report. Get a copy of the police report(s) as it may be necessary to provide a copy to your creditors to clear your records.

The Federal Trade Commission provides important information on its website on identity theft, how it can be prevented and what to do if you suspect you have been the victim of such a theft. The website address for the FTC site is as follows:

http://www.ftc.gov/bcp/edu/microsites/idtheft//

(Facilities must check this site before sending out any notices to ensure that the credit reporting agency phone numbers have not changed. If any changes have been made, the correct numbers must be inserted in this letter.)

You should check this website for additional information on steps you should take (such as closing any accounts you did not open).

Please know that the Hawaii Health Systems Corporation takes the (*loss **or** theft **or** unauthorized access*) of this information very seriously and regrets any problems this incident may cause you. We have taken the following measure to secure the data (*generally describe the measures you have taken—Do NOT describe measures that, if made public, could hamper security*) If there are any further questions our department can assist you with, please contact _____ at _____.

Protection of Personnel Information
Report to the Legislature
Sample Transmittal Letter

NOTE: All breaches involving ***personal information*** *must be reported to the Legislature. (Breaches involving personnel information that do NOT contain personal information are NOT reported to the Legislature.) The breaches must be reported within 20 days after the discovery of the breach, unless a law enforcement agency asks the department to delay the notice to affected individuals. If there is a request from law enforcement to delay the notice, the report to the legislature must be made within 20 days after the law enforcement agency determines that the notice will no longer impede the investigation or jeopardize national security.*

The notice must be sent to both the House and Senate

The Honorable _____
and Members of the Senate (or House of Representatives)
State Capitol
Honolulu, Hawaii 96813

Dear President (or Speaker) _____ and Members of the Senate (or House):

In accordance with Section 487N-4, Hawaii Revised Statutes, the HHSC's _____ (*Facility Name*) is reporting a breach of personal information.

This breach involved (*describe the nature of the breach*).

The breach involved information on (*state the number of individuals affected by the breach*) individuals and (*all* ***or*** *state the number of individuals to whom notices were sent*) were sent a copy of the attached notice. The notice to affected individuals (*was* ***or*** *was not*) delayed at the request of a law enforcement agency.

We take the protection of personnel information very seriously. Accordingly we have taken the following measures to prevent any recurrence of the breach (*generally describe the measures you have taken—Do NOT describe measures that, if made public, could hamper security*).

If you have any questions regarding this matter, please contact _____ at _____.

Attachment

cc:
Miles Takaaze, VP Communications/Public Affairs Director
Janice Wakatsuki, VP/Director of Human Resources
Rene McWade, VP/General Counsel
Barbara Kahana, CP/IT
Corporate HR

Protection of Personnel Information
Report to the Office of Consumer Protection
(Breaches Involving Personal Information of 1,000 or more individuals only)

_____, Executive Director
Office of Consumer Protection
235 South Beretania Street, Room 801
Honolulu, Hawaii 96813

Dear _____:

In accordance with Section 487N-2, Hawaii Revised Statutes, _____ (Facility Name) is reporting a security breach involving the personal information of _____ (*number of individuals—must be over 1,000 or this letter is NOT required*) individuals.

As required by law, we are notifying these individuals by the following means (*in writing, via email, phone* ***and/or*** *via substitute notice*). The notices (*will be* ***or*** *have been*) sent out on _____. A copy of the notification is attached for your information.

If you have any questions related to this incident, please contact _____ at _____.

Attachment

cc: Janice Wakatsuki, VP/Director of Human Resources
Rene McWade, VP/General Counsel
Corporate HR

Protection of Personnel Information
Report to the Credit Bureaus
(Breaches involving Personal Information 1,000 or more individuals only)

Send the following notice to each of the three credit reporting agencies listed in the notice to employees. Check the FTC website for the current address for each agency.

Dear _____:

In accordance with Section 487N-2, Hawaii Revised Statutes, the Hawaii Health Systems Corporation, _____ () is reporting a security breach involving the personal information of _____ (*number of individuals—must be over 1,000 or this letter is NOT required*) individuals.

As required by State of Hawaii law, we are notifying these individuals by the following means (*in writing, via email, phone* ***and/or*** *via substitute notice*). The notices (*will be* ***or*** *have been*) sent out on _____. A copy of the notification is attached for your information.

If you have any questions related to this incident, please contact _____ at _____.

Attachment

cc: Janice Wakatsuki, VP/Director of Human Resources
Rene McWade, VP/General Counsel
Corporate HR