HAWAII HEALTH SYSTEMS CORPORATION *Quality Healthcare for All* **PROCEDURE**	**Department:** **HUMAN RESOURCES**	**Procedure No.:** **HR 0010B** **Supersedes Procedure No.:**
Subject: **Protection of Personnel Information Program**	**Approved By:** Linda Rosen By: Linda Rosen, M.D., M.P.H. Its: President & CEO	**Approved Date:** January 27, 2022 **Last Reviewed:** October 11, 2021

I. PURPOSE:

To establish procedures to prevent identity theft of HHSC applicants and employees and to comply with State laws involving the use, protection and destruction of Personal Information.

II. PROCEDURES:

A. Vice President and Chief Human Resources Officer

The Vice President and Chief Human Resources Officer (VP&CHRO) shall be responsible for:

1. Designating a lead position in the HHSC Corporate Human Resources Department to be responsible for managing the protection of personnel information program.

    a. The designated position is: Human Resources Information Systems Manager (HRISM).

    b. In the event that the HRISM is unavailable, the Assistant Director of Human Resources shall be the responsible designee.

2. Promulgating and maintaining procedures and guidelines intended to secure Personnel Information and comply with federal and state laws related to the Protection of Personal Information — including social security numbers.

3. Coordinating the regional Human Resources Departments' efforts to comply with federal and state law related to the protection of Personnel Information — including answering questions related to the law.

4. Auditing (as deemed necessary by the VP&CHRO) regional compliance with the procedures and federal and state laws.

5. Ensuring proper notification is provided to any employee in the event of a security Breach of Personnel Information.

B. Information Technology Department ("ITD")

The ITD shall be responsible for:

1. Ensuring that appropriate electronic data security programs and policies are established.

2. Ensuring that the Director of Information Technology Security is responsible for IT Security for HHSC.

3. Ensuring that all requests to ITD for Personnel Information on electronic media or printed hard copy are authorized in writing by the VP&CHRO.

4. Ensuring that any Security Breach is reported and investigated by the Director of IT Security. Security Breaches and Personnel Information breaches shall be reported to the VP&CHRO and the HRISM.

C. Each Regional Chief Human Resources Officers ("RCHRO")

The RCHRO shall be responsible for:

1. Coordinating the protection of use, protection, and destruction of Personnel Information collected and maintained for the region.

2. Authorizing and maintaining a list of employees who are authorized to handle and view Personnel Information in the region.

3. Ensuring that the procedures to secure Personnel Information and to comply with federal and state laws are followed, which shall include 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 Security Breach and notifying the Director of IT Security for Security Breaches involving IT related issues.

5. Cooperating with the Corporate HR Office in its efforts to ensure compliance with federal and state law related 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:

1. Treating all Personnel Information the employee handles or becomes aware of as confidential (unless the information is expressly covered by federal or state laws deeming the information to be public information). 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 shall apply.

2. Disclosing personnel information only when authorized to do so by the VP&CHRO or RCHRO and only to those individuals who are authorized to receive the information. Unauthorized written and oral communication of Personnel Information and Personal Information is strictly prohibited.

    a. Authorized disclosure may be obtained via a written and signed request from an employee to disclose his/her records. Such requests should be reviewed by the RCHRO and may be reviewed by the Vice President and General Counsel (VP&GC) or his/her designee and the disclosure should only be for the records as expressly authorized.

    b. Authorized disclosure may also be by normal processing procedures. In the event that the forms contain Personal Information, no other specific authorization shall be required. Each HR Department shall ensure that all confidential transmittals protect the confidentiality of the information, e.g.,

hand carrying the documents or placing the documents in a sealed envelope marked “confidential.” Transmittals shall include but not be limited to procedures such as processing Employee Transactions Report (ETR), Employee-Union Trust Fund (EUTF), and payroll electronic files.

c. Authorized disclosures may be made where a collective bargaining agreement requires the disclosure of the Confidential Information. The VP&CHRO or the RCHRO shall be consulted prior to the disclosure.

d. Authorized disclosures may be necessary to respond to a subpoena or court order for Personnel Information. The responsible VP&CHRO or RCHRO shall be consulted before such a disclosure is made. The VP&CHRO and the RCHRO may also consult with Legal Counsel prior to authorizing disclosure.

3. All employees who are authorized to handle and those who work with, Personnel Information shall be on alert for possible Information Breach. If an Information Breach or Security Breach are detected, the individual shall immediately notify the VP&CHRO or the responsible RCHRO to ensure that necessary and required actions are taken to secure the Confidential Information and to ensure that the breach is handled in accordance with required procedures and applicable federal and state law. After notifying the VP&CHRO or the responsible RCHRO, the employee shall treat information related to the Information Breach or Security Breach (or both) as confidential. Disclosure of the breach prior to the completion of required investigations could 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 Confidential Information or to otherwise comply with the policy and this procedure. Disciplinary action shall be in accordance with the respective collective bargaining agreements and the HHSC Human Resources and Civil Service System Rules, as applicable.

C. PROTECTION OF CONFIDENTIAL INFORMATION — GUIDELINES

It is recognized that one of the best ways to protect Confidential Information is to NOT collect and/or provide the information unless it is required by law or otherwise deemed necessary. Accordingly, the VP&CHRO and the respective RCHRO shall periodically review those personnel practices that require the collection of Personal Information and shall determine whether the collection of such information necessary and if not ensure that the practice is stopped.

1. Protection of Paper Records

   a. All HR offices shall have locked storage cabinets of some type to secure personnel files and records that need to be available to authorized employees.

   b. Personnel folders for employees who have separated from service shall be delivered to the State Records Center, to which access is restricted, by the VP&CHRO and the respective RCHROs.

   c. Personnel records that contain Confidential Information and that are not being actively worked on shall be stored in locked file cabinets or desks. This includes, but is not limited to:

      1) Personnel related forms that contain social security numbers, such as personnel action forms (Lawson ETR forms), ERS forms, and EUTF forms; and

2) Individual personnel records that do not contain Personal Information, may still contain Confidential Information and other sensitive information, e.g., home addresses, which shall be protected from disclosure in the same manner.

d. Employees actively working on a personnel file shall be responsible for protecting such documents. If the individual leaves his/her desk,

1) The record shall be secured by locking it in their desk or filing cabinet in an area with limited access, or locking the record in their secured office.

2) 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.

2. Protection of Electronic Records

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

a. Adherence to the policies and procedures established by HHSC's ITD for data security, computer system back up, and the use of internet and email is required by all individuals who handle personnel information.

b. Employees shall secure the computers on which they view Confidential Information in accordance with all applicable IT policies and procedures. This includes, but is not limited to, password protection to log on to the computer and setting the screen saver to come on after a short period of inactivity.

1) Employees shall take special precautions with laptop computers and shall NOT store Personnel Information on personal computers that contain their own personal information.

2) Employees shall not leave laptop computers containing Personnel Information unattended.

c. Employees shall not place or store Confidential Information on removable devices and media such as flash drives, CDs, DVDs, tapes, or diskettes unless authorized according to HHSC's standard processing procedures. All such Confidential information shall be encrypted (NOT just password protected).

1) Without prior approval from the VP&CHRO or responsible RCHRO, employees shall not place large amounts of Confidential Information onto these devices.

2) The VP&CHRO or responsible RCHRO may approve an exception if the information is required for the employee's job and a removable device is necessary. The employee, having custody of such data, shall secure the removable device and the data in accordance with the applicable IT policies and procedures.

d. Employees shall not store Personnel Information in electronic folders on file servers that are accessible to unauthorized employees.

e. Employees shall take precautions to secure Personnel Information when faxing or emailing documents. Unless absolutely necessary, Personal

Information shall not be sent by fax or email, and then only if the document is sent to a secured location accessible by authorized personnel only.

3. Special Precautions for Social Security Numbers

   a. Chapter 487J, Hawaii Revised Statutes (HRS) provides special protection for social security numbers. While state 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 deems the social security number as highly Confidential Information that shall be afforded proper protection. In the event that certain use and disclosure of social security numbers falls outside of the strict employment context, the RCHROs shall review and comply with state and federal law when social security numbers are collected, used or disclosed.

   b. The following are recommended practices related to the use of social security numbers.

      1) 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&CHRO. If an exception has been made, the file must, at a minimum, be password protected.

      2) If a social security number must be used, whenever possible, only the last four digits should be used.

      3) Social security numbers are not to be printed or imbedded on any employee identification card or any other card required for access.

      4) 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).

      5) 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.

D. NOTIFICATION OF BREACH

Pursuant to Chapter 487N, HRS, HHSC is required to notify affected individuals when it is discovered or it is notified of a Security Breach or Information Breach or both. The VP&CHRO and each RCHRO shall be responsible for ensuring compliance with the notification requirements set forth in Chapter 487N. Additionally, depending on the specific facts, the VP&CHRO 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).

VP&CHRO or the responsible RCHRO shall provide the applicable notification letters or forms, attached hereto as Attachments 2 through 7.

E. DISPOSAL OF INFORMATION

Personnel Information shall also be protected when the record retention schedule requires destruction of paper or non-paper (such as electronic) document or files or media.

1. Paper Documents

   All paper documents containing Personnel Information or Personal Information shall be destroyed in such a manner that the information contained in the document(s) cannot practicably be read or reconstructed. The following methods of destruction, in addition to State of Hawaii, Department of Accounting and General Services' (DAGS) - General Records Schedule and disposal procedures, are considered acceptable:

   a. Burning. A representative of the facility controlling the records shall witnesses the documents being burned.

   b. Pulverizing. A representative of the facility controlling the records shall witness the pulverizing of the documents.

   c. Shredding. If not personally shredding the documents, a representative of the facility controlling the records shall serve as the witness.

2. Electronic Documents

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

3. 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 record destruction. Facilities electing to use such a company shall ensure that all requirements of the law are met including the transfer of such records to the contractor.

F. TRAINING AND CERTIFICATION OF RECEIPT OF MATERIALS

1. Corporate HR and/or the Regional HR offices shall offer training to employees who are authorized to handle Confidential Information. This training shall be conducted during new hire orientation and any additional training as deemed necessary.

2. Corporate HR and/or the Regional HR office shall offer refresher training, as deemed necessary, for employees who are authorized to handle Confidential Information.

3. Whether or not an employee who is authorized to handle Confidential Information has completed the training, the employee shall be provided with a copy of this policy.

4. Employees who have read and/or received a copy of this policy shall acknowledge that they have read the policy and understand the confidentiality requirements contained herein by signing the Certificate of Understanding form, attached hereto as Attachment 1.

III. ATTACHMENT(S):

Attachment 1: Certificate of Understanding
Attachment 2: Law Enforcement Request to Delay Notification
Attachment 3: Law Enforcement Request to Delay Notification Agency — Documentation of Request
Attachment 4: Notification to Affected Individuals Breaches Involving Personal Information
Attachment 5: Report to the Legislature Sample Transmittal Letter
Attachment 6: Report to the Office of Consumer Protection (Breaches Involving Personal Information of 1,000 or more individuals only)
Attachment 7: Report to the Credit Bureaus (Breaches involving Personal Information 1,000 or more individuals only)

Facility: ****

Department: _____

Authorization to Handle Personnel Information
Protection of Personnel Information
Certificate of Understanding (the "Certificate")

I acknowledge that I have been provided an electronic, hard copy or have read completely the Protection of Personnel Information Program (the "Program") policy and procedure and related documents. 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 responsible for reviewing the materials and strictly complying with the Program. I further understand that I am 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 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 shall immediately contact _____ (or his/her successor or designee), the Regional Chief Human Resources Officer 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 Chief Human Resources Officer (or his/her successor or designee).

_____ _____
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 individuals of the breach or suspected breach reported on _____ regarding
Agency Reporting the Breach

_____
(Describe the Breach)

_____

at this time notification may impede a criminal investigation or jeopardize national security. I will notify the agency promptly when notifying the affected individual(s) 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 Documentation of Request shall be used to document that a verbal request to delay notification of breach (or suspected breach) until the law enforcement officer completes the written request. (The department shall make every effort to obtain written confirmation of the request.)

The following information shall beat the same time that the request for delay of notification is made by a representative of a 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:

Law Enforcement Agency for whom Requestor Works _____

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

*Note: The Vice President and Chief Human Resources Officer 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 personal information. The incident (*describe the incident in general terms*). The information that (*has been **or** is suspected of being*) (*lost **or** stolen **or** acquired or disclosed*) 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 state 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, e.g., your home address, social security number, your employer information, and any other relevant information are correct. 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 Personal Information
Report to the Hawaii State Legislature
Sample Transmittal Letter

*NOTE: All breaches involving **personal information** shall be reported to the Hawaii State Legislature. (Breaches involving personnel information that do NOT contain personal information are NOT reported to the Legislature.) A breach must be reported within twenty (20) days after the discovery of the breach, unless a law enforcement agency asks the department to delay notification to the affected individual(s). 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.

HHSC takes the protection of personal information very seriously. Accordingly the following measures to prevent any recurrence of the breach have been taken (*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: HHSC President & Chief Executive Officer (PCEO)
Regional Chief Executive Officer (RCEO)
VP & CHRO
VP & General Counsel
RCHRO
VP & CIO
Corporate HR

Protection of Personal 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, HHSC is notifying these individuals of the breach 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: VP & CHRO
VP & General Counsel
Corporate HR

Protection of Personal 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 that were listed in the Notification to Affected Individuals. 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, _____ (HHSC) 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, HHSC is 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: VP & CHRO
VP & General Counsel
Corporate HR