RCUH Research Corporation of the University of Hawai'i

3.950 RCUH Destruction of Personal Information

I. Policy

It is the RCUH's policy to ensure all sensitive/personal information is handled carefully and responsibly in order to avoid being abused for improper and/or illegal activities. It is also to comply with the Hawaii Revised Statutes, Chapter 487R which requires all employers to take reasonable measures to protect against unauthorized access of sensitive information in connection with disposal of documents and records.

This policy provides a description of procedures relating to:

1) The security and protection of sensitive/personal information, and;

2) The adequate destruction or proper disposal of records, documents, electronic media, and other non-paper media containing sensitive/personal information.

II. Applications

RCUH employees working for University of Hawaii (UH) projects are subject to Confidentiality and Security Policies and Procedures applicable to their respective University, College, Institute or other applicable UH entity.

RCUH employees working for non-University of Hawaii projects are subject to Confidentiality and Security Policies and Procedures of that business entity.

In the absence of any policy, this policy shall apply to all RCUH employees, who, in the course of their employment, have access to, handle, store, and/or dispose of or transfer paper documents, electronic media, or other media containing sensitive and/or personally identifiable information.

This policy also applies to all Principal Investigators and/or designees who employ individuals through the RCUH.

III. Responsibilities

A. RCUH Employee

a. Read and sign the Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form to signify your understanding of your responsibilities under this policy

b. Follow the prescribed procedures defined in the "procedures" section above if job duties require access to, handling, storage and/or disposal of sensitive information

c. Notify the RCUH Director of Human Resources or Principal Investigator of any violation of this policy, or of any concerns regarding the secure disposal or destruction of sensitive information

B. Principal Investigator

a. Responsible for overall security, protection and proper destruction of sensitive information in accordance with the procedures described above

b. If any type of Personal Information "System" is maintained, complete an annual "Personal Information Systems Survey"

c. Notify the RCUH Director of Human Resources of any violation of this policy, or of any concerns regarding the secure disposal or destruction of sensitive information

IV. Details of Policy

A. Definitions Relating to Sensitive/Personal Information:

a. **Sensitive/Personal Information:** (Herein referred to as "Sensitive information") is information that is subject to privacy considerations or has been classified as confidential and subject to protection from public access or inappropriate disclosure. It includes, but is not limited to:

i. Social Security Number, Home and mailing address, Home phone number, Date of Birth/Age, Ethnicity, etc.
ii. Health/Medical records including anything covered by the Health Insurance Portability and Accountability Act (HIPAA)
iii. Job applicant records (Names, transcripts, etc.)
iv. Employment and payroll records
v. UH Usernames, passwords, "secret questions and answers" or other ID/password combinations for applications that contain or use personally identifiable information
vi. Credit card, debit card or credit-related information
vii. Bank account information

b. **Electronic and Other Media:** Includes any non-paper material or media on which information can be stored or preserved, including, but not limited to, computers, laptops, notebooks, tablet computers, phones, computer hard drives, zip drives, "thumb" drives, floppy disks, USB flash drives, memory sticks, magnetic tape, or other electromagnetic or electromechanical means of storing data, and includes optical storage media such as CDs or DVDs. It shall also include items such as identification cards, credit cards, or other non-paper material containing personal information.

B. **Security and Protection of Sensitive/Personal Information:** Confidentiality of sensitive/personal information is protected by Chapter 92F (Uniform Information

Practices Act) of the Hawaii State Revised Statutes, the Federal Privacy Act of 1974, and other applicable state and federal laws. It is each employee's responsibility to respect and protect the confidentiality of such information.

a. **Access to Sensitive Information:** Access to sensitive information should be limited and granted to individuals on a "need-to-know" basis only, and only when it is necessary for the completion of the employee's job responsibilities.

b. **Transmission of Sensitive Information:** Senders of sensitive information must take care to protect the information and inform the recipient(s), including those involved in the delivery of the process, that the transmission contains sensitive information and must be protected.

c. **Use of Sensitive Information:**

   i. Accessing or seeking to gain access to sensitive information except in the course of fulfilling an employee's job responsibilities is prohibited.
   ii. Disclosing, using or altering any such information without proper authorization is prohibited.
   iii. Employees must keep login information to systems containing sensitive information confidential unless directed by the Principal Investigator. Employees should exercise caution while using public computers and networks, especially for storing and/or accessing their login, password, and/or other sensitive information. Using other individual's login information is also prohibited unless given explicit permission to do so to resolve a reported problem.
   iv. Transactions processed on the project's Information Systems may be automatically logged, and subject to review as part of information security assurance

d. **Storage of Sensitive Information**

   i. **Electronic Storage of Sensitive Information:** Systems on which sensitive information is stored must minimally comply with all basic computer security standards (i.e. patch management, anti-virus protection, password controls, etc.). Sensitive information stored on any system/media (including, but not limited to laptops, notebooks, USB drives, diskettes, CD/DVDs, personal computers, mobile devices, phones) must be password protected and encrypted whenever not in active use.

   ii. **Paper Storage of Sensitive Information:** Paper documents and files containing sensitive information must be secured when not in

active use in a secure environment with access limited to authorized users.

C. **Responsibility and Oversight of the Destruction of Sensitive/Personal Information:**

a. **Principal Investigator is Responsible for the Proper Destruction of Sensitive Information Maintained at the Project:** Principal Investigators are responsible for the proper destruction of sensitive information however the Principal Investigator may designate an individual to be responsible for oversight of the destruction of personal information. His/her responsibilities will include:

i. Identifying employees who handle and/or dispose of documents or electronic or other media containing personal information.
ii. Providing appropriate guidelines to ensure compliance that all documents/records containing personal information is disposed of in a proper manner (as described below).
iii. Conducting due diligence on any destruction services provided by a third party.

D. **Annual Reporting of Personal Information Systems:** As required by Hawaii State Law (HRS 487N), every state agency is required to identify all information systems that maintain personal information. Therefore, each Principal Investigator who maintains any type of "Personal Information System" must complete an annual survey administered by the RCUH (for Direct Projects) and University of Hawaii. (for UH Service Ordered Projects)

a. **"Personal Information System" Definition:** For purposes of this annual requirement, a "Personal Information System" is a system containing: 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:

i. Social security number (unless redacted to the last four digits):
ii. Driver's license number or Hawaii identification card number; or
iii. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account such as a bank account, checking account, retirement/pension account, brokerage account, etc.

b. **Examples of Common Electronic and/or Paper-based Systems:**

i. Personnel files of project employees
ii. Worker's Compensation files
iii. Employment records of employees (i.e. emergency contact listing, car/parking information)
iv. Fiscal or payroll reports/records

v. Procurement files/records (i.e. travel, purchasing payment records, contracts)
vi. Accounting records
vii. Patient data for research

E. **Compromise of Sensitive Information:** In the event login information and/or sensitive information have been compromised, the user must notify his/her respective Principal Investigator and/or the responsible Information Systems Security Officer.

F. **Violations of this Policy:** Violations of this policy may result in disciplinary action up to and including termination of employment. Violators may also be subject to applicable civil and/or criminal penalties

V. Procedures

A. **Procedures for the Proper Transfer of Sensitive Information:**

a. **Transmission of Sensitive Information:** Senders of sensitive information must take care to protect the information and inform the recipient(s) that the transmission contains sensitive information and must be protected.
b. **Paper Transmissions:** When transmitting sensitive information on paper, the sender should mark the envelope as "CONFIDENTIAL" as appropriate to minimize the chance of unnecessary exposure.
c. **Electronic Transmissions:** When possible, sensitive information should be encrypted when it is being transmitted over public networks or carriers in electronic form (i.e. email, file transfers, web transactions, or instant messaging).
d. **Fax Transmissions:** When sending sensitive information via facsimile, the sender should ensure that the information is promptly received and properly protected at both the sending and receiving location.

B. **Procedures for Proper Destruction of Sensitive Information on Paper:**

a. **Review of Documents or Electronic and Other Media Prior to Disposal:** Prior to disposing of documents or electronic and other media by any non-secure method, individuals who dispose of documents or electronic and other media containing personal information must review it to ensure that it does not contain sensitive information as defined by this policy.
b. **Destruction Procedures for Paper Documents:** All employees disposing of paper documents, microfilm, photographs, negatives, and similar media which contain sensitive information must do so by one of the following methods:
i. **Dispose of Paper Documents by Project Staff/Employees:** If disposing of documents containing sensitive information through shredding or pulverizing, the responsible individual must check the document after destruction to determine whether the sensitive information can be read. If so, the document should be re-shredded, cross-shredded, or re-pulverized, and checked again. If the document cannot be shredded or

pulverized so as to make its contents unreadable, the document should be set aside for burning or other destruction methods. Contact the RCUH Human Resources Department for further instructions or guidance.

ii. **Documents to be destroyed by Service Provider:** A third-party for document destruction services may be obtained. In this case, the documents are placed in secure disposal containers for disposal by the destruction service provider. The project/program administrator will be responsible to ensure the third party has the means to comply with the Hawaii Destruction of Personal Information Law. This normally requires a certification from the vendor and a receipt of all records destroyed. These certifications and receipts must be kept in the project/program office.

C. **Procedures for Proper Destruction of Sensitive Information on Electronic Media:** An employee disposing of electronic media, or non-paper and non-electronic media containing sensitive information shall do so by one of the following methods:

a. **For Computers, Servers, Phones, and PDA, Notebooks, Tablet Computer Devices:**

i. Before these devices are sold, leased, donated, recycled, or otherwise transferred to a third party for further use, the hard drive(s) shall be erased and reformatted using a software program designed to ensure the secure destruction of sensitive information or removed from the unit.

ii. If sensitive information cannot be securely erased from the device, the hard drive or other component containing the sensitive information shall be securely destroyed by a third party vendor certified to perform this type of physical destruction.

iii. If these devices containing sensitive information is to be disposed of, rather than transferred to a third party for further use, the hard drive(s) of the device and any recording or memory unit of the device containing sensitive information shall either be physically removed and destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.

b. **For Storage Media (i.e. Zip Drives, Disks, Flash Drives, Optical Storage Media, etc.):**

i. Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing sensitive information shall have the data contained in the item destroyed by either wiping the media with a degaussing magnet, or by physically destroying the media through shredding or similar physical destruction. CD's, DVD's, and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.

ii. Disposal may also be accomplished by providing the electronic storage media or optical storage media to a third-party destruction.

c. **For Non-Paper and Non-Electronic Media:**

i. Sensitive information may be recorded on non-paper and non-electronic media such as plastic identification cards, credit cards, celluloid film, etc. If such media consists of material (such as plastic credit cards) suitable for shredding or pulverizing, disposal should be accomplished in the same manner as paper documents.
ii. If such media is not suitable for shredding or pulverizing, an employee disposing of such media must be destroyed by a third party vendor certified to perform this type of physical destruction.

D. **Annual Reporting of Personal Information Systems:** Each Principal Investigator who maintains any type of Personal Information "System" must complete an annual survey (conducted in September of each year).

   a. **For Direct Projects to the RCUH**: A Personal Information Systems Survey must be completed/updated and submitted to the RCUH Human Resources Department by the established deadlines.
   b. **For University of Hawaii Service Ordered Projects**: An online survey (administered by the University of Hawaii System Office) must be completed/updated by the established deadlines.Surveys may be entered/accessed by going to:http://www.hawaii.edu/its/information/survey/

E. **Employees Must Sign Acknowledgment Form**: Upon hire, new hires must read and sign the Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form to signify their understanding of their responsibilities under this policy.

F. **Employees Must Report of Violations of This Policy**: Employees should immediately notify the RCUH Director of Human Resources or their Principal Investigator/Designee of any violation of this policy, or of any concerns they may have regarding the secure disposal or destruction of sensitive information.

VI. Contact

RCUH Administration: (808) 956-3100
rcuhhr@rcuh.com

VII. Relevant Document

Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form

Chapter 92F (HRS)

Federal Privacy Act of 1974

Hawaii Revised Statutes, Chapter 487R

Hawaii State Law (HRS 487N)

http://www.hawaii.edu/its/information/survey/

Date Revised: 03/17/2011, 04/18/2016, 06/27/2018, 08/13/2018, 07/24/2019