

to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Dispensary CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Dispensary CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Dispensary Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

## **2.7 TRANSFER OF SENSITIVE/CONFIDENTIAL INFORMATION**

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Dispensary and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Dispensary policy and will result in personnel action, and may result in legal action.

## **2.8 TRANSFERRING SOFTWARE AND FILES BETWEEN HOME AND WORK**

Personal software shall not be used on Dispensary computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Dispensary purchased software on home or on non-Dispensary computers or equipment.

Dispensary proprietary data, including but not limited to patient information, IT Systems information,

## **2.9 INTERNET CONSIDERATIONS**

Special precautions are required to block Internet (public) access to Dispensary information resources not intended for public access, and to protect confidential Dispensary information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Dispensary Privacy Officer or appropriate personnel authorized by the Dispensary shall be obtained before:

- An Internet, or other external network connection, is established;
- Dispensary information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the Dispensary. The network can be used to market services related to the Dispensary, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.

## **2.10 INSTALLATION OF AUTHENTICATION AND ENCRYPTION CERTIFICATES ON THE E-MAIL SYSTEM**

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

## **2.11 USE OF WINZIP ENCRYPTED AND ZIPPED E-MAIL**

PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

HALE MAKAI'IKE (HMI)		Policy and Procedure	
Title: IDENTIFICATION and AUTHENTICATION		P&P #: IS-1.2	
		Review: Annual	
		Information Technology	

## 3 Identification and Authentication

---

### 3.1 USER LOGON IDS

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are yearly and all inactive logon IDs are revoked. The Dispensary Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of Ten (10) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Dispensary systems or networks must have a completed and signed Network Access Form (Appendix C). This form must be signed by the supervisor or department head of each user requesting access.



Change Frequency – Passwords must be changed every 180 days. Compromised passwords shall be changed immediately.

Reuse - The previous 3 passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

### **3.3 CONFIDENTIALITY AGREEMENT**

Users of Dispensary information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix D). The agreement shall include the following statement, or a paraphrase of it:

*I understand that any unauthorized use or disclosure of information residing on the Dispensary information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Dispensary information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

### **3.4 ACCESS CONTROL**

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.)

## **Identification and Authentication Requirements**

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

### **3.5 USER LOGIN ENTITLEMENT REVIEWS**

If an employee changes positions at the Dispensary, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Network Access Request Form (Appendix C) both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

No less than annually, the IT Manager shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect patient data.

### **3.6 TERMINATION OF USER LOGON ACCOUNT**

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by indicating "Remove Access" on the employee's Network Access Request Form (Appendix C) and submitting the Form to the IT Department. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled work day so that their user account(s) can

HALE MAKAIKE (HMI)		Policy and Procedure	
Title: NETWORK CONNECTIVITY		P&P #: IS-1.3	
		Review: Annual	
		Information Technology	

## 4 Network Connectivity

---

### 4.1 DIAL-IN CONNECTIONS

Access to Dispensary information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrants additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

### 4.2 DIAL OUT CONNECTIONS

Dispensary provides a link to an Internet Service Provider. If a user has a specific need to link with an

- conference calling contracts
- cell phones
- Smart Phone type devices
- call routing software
- call reporting software
- phone system administration equipment
- Fiber/Network lines
- long distance lines
- local phone lines
- PRI circuits
- telephone equipment

#### **4.4 PERMANENT CONNECTIONS**

The security of Dispensary systems can be jeopardized from third party locations if security dispensaries and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required the value of the information, the security measures employed by the third party, and the implications for the security of Dispensary systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

#### **4.5 EMPHASIS ON SECURITY IN THIRD PARTY CONTRACTS**

Access to Dispensary computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Dispensary Information Security Policy have been reviewed and considered.
- Policies and standards established in the Dispensary information security program have been

- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreed upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

## 4.6 FIREWALLS

Authority from the Manager of Information Systems or appropriate personnel must be received before any employee or contractor is granted access to a Dispensary router or firewall.

HALE MAKAI'IKE (HMI)		<b>Policy and Procedure</b>
<b>Title: MALICIOUS CODE</b>	<b>P&amp;P #: IS-1.4</b>	
	<b>Review: Annual</b>	
	<b>Information Technology</b>	

## 5 Malicious Code

---

### 5.1 ANTIVIRUS SOFTWARE INSTALLATION

Antivirus software is installed on all Dispensary personal computers and servers. Virus update patterns are updated daily on the Dispensary servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by the Dispensary is Symantec End Point Protection<sup>18</sup>. Updates are received directly from Symantec<sup>19</sup> which is scheduled daily at 5:00 PM<sup>20</sup>.

Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Dispensary network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

### 5.2 NEW SOFTWARE DISTRIBUTION

Only software created by Dispensary application staff, if applicable, or software approved by the Privacy

All data and program files that have been electronically transmitted to a Dispensary computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Dispensary personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Dispensary computer or network.

Computers shall never be “booted” from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD\_ROM, DVD or USB device is not “bootable”.

### **5.3 RETENTION OF OWNERSHIP**

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Dispensary are the property of the Dispensary unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Dispensary ownership at the time of employment. Nothing contained herein applies to software purchased by Dispensary employees at their own expense.

HALE MAKAI'IKE (HMI)		Policy and Procedure	
Title: ENCRYPTION		P&P #: IS-1.5	
		Review: Annual	
		Information Technology	

## 6 Encryption

---

### 6.1 DEFINITION

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

### 6.2 ENCRYPTION KEY

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Dispensary shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. The Dispensary employs several methods of secure data transmission.

### 6.3 INSTALLATION OF AUTHENTICATION AND ENCRYPTION



## **6.5 FILE TRANSFER PROTOCOL (FTP)**

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

## **6.6 SECURE SOCKET LAYER (SSL) WEB INTERFACE**

Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

HALE MAKAI'IKE		Policy and Procedure	
Title: RETENTION / DESTRUCTION of PAPER DOCUMENTS		P&P #: IS-1.9	
		Review: Annual	
		Information Technology	

## 7 Retention / Destruction of Medical Information

---

Many state and federal laws regulate the retention and destruction of medical information. The Dispensary actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information dispensary, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 7 Years.

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST 800-88 guidelines.

HALE MAKAIKE		Policy and Procedure	
Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE		P&P #: IS-1.10	
		Review: Annual	
		Information Technology (TVS020, TVS021)	

## 8 Disposal of External Media / Hardware

---

### 8.1 DISPOSAL OF EXTERNAL MEDIA

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

HALE MAKAI'IKE		Policy and Procedure	
Title: CHANGE MANAGEMENT		P&P #: IS-1.11	
		Review: Annual	
		Information Technology	

## 9 Change Management

---

### Statement of Policy

To ensure that Dispensary is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contains electronic protected health information ("ePHI"). Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

### Procedure

1. The IT staff or other designated Dispensary employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
  - a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or electronic health record (EHR) updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are

HALE MAKAI'IKE		Policy and Procedure	
Title: AUDIT CONTROLS		P&P #: IS-1.12	
		Review: Annual	
		Information Technology	

## 10 Audit Controls

---

### Statement of Policy

To ensure that Dispensary implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information ("ePHI"). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Dispensary is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Dispensary will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

### Procedure

1. See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.
2. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store ePHI for purposes of generating audit logs. Each audit log shall include, at

HALE MAKAI'IKE		Policy and Procedure	
<b>Title: INFORMATION SYSTEM ACTIVITY REVIEW</b>		<b>P&amp;P #: IS-1.13</b>	
		<b>Review: Annual</b>	
		<b>Information Technology</b>	

## 11 Information System Activity Review

---

### Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Dispensary shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

### Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Dispensary's information systems that contain or use ePHI.
2. The Information Technology Services shall be responsible for conducting reviews of Dispensary's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible,

- c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
- d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.

1. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Dispensary's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).



HALE MAKAI'IKE (HMI)		<b>Policy and Procedure</b>
<b>Title: DATA INTEGRITY</b>	<b>P&amp;P #: IS-1.14</b>	
	<b>Review: Annual</b>	
	<b>Information Technology</b>	

## 12 Data Integrity

---

### Statement of Policy

Dispensary shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect Dispensary's ePHI from improper alteration or destruction.

### Procedure

To the fullest extent possible, Dispensary shall utilize applications with built-in intelligence that automatically checks for human errors.

Dispensary shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, Dispensary will use encryption, as determined to be appropriate, to preserve the integrity of data.

Dispensary will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, Dispensary will test its information systems for accuracy and

HALE MAKAI'IKE (HMI)		<b>Policy and Procedure</b>
<b>Title: CONTINGENCY PLAN</b>	<b>P&amp;P #: IS-1.15</b>	
	<b>Review: Annual</b>	
	<b>Information Technology</b>	

## 13 Contingency Plan

---

### Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI.

Dispensary is committed to maintaining formal dispensaries for responding to an emergency or other occurrence that damages systems containing ePHI. Dispensary shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

### Procedure

1. Data Backup Plan
  - a. Dispensary, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.
  - b. At the conclusion of each day, Monday through Sunday, a full backup of all servers containing ePHI shall be backed up to tape.
  - c. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

- ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.
- b. The disaster recovery and emergency mode operation plan shall include the following:
  - i. Current copies of the information systems inventory and network configuration developed and updated as part of Dispensary's risk analysis.
  - ii. Current copy of the written backup procedures developed and updated pursuant to this policy.
  - iii. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.
  - iv. Identification of an emergency response team. Members of such team shall be responsible for the following:
    - 1. Determining the impact of a disaster and/or system unavailability on Dispensary's operations.
    - 2. In the event of a disaster, securing the site and providing ongoing physical security.
    - 3. Retrieving lost data.
    - 4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
    - 5. Taking such steps necessary to restore operations.

4. All current workforce members.

c. The disaster recovery team shall meet on at least an annual basis to:

- i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Dispensary;
- ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and
- iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

HALE MAKAI'IKE (HMI)		<b>Policy and Procedure</b>
<b>Title: SECURITY MANAGEMENT PROCESS</b>	<b>P&amp;P #: IS-1.17</b>	
	<b>Review: Annual</b>	
	<b>Information Technology</b>	

## 14 Security Management Process

---

### Statement of Policy

To ensure Dispensary conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Dispensary.

Dispensary shall conduct an accurate and thorough risk analysis to serve as the basis for Dispensary's HIPAA Security Rule compliance efforts. Dispensary shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business dispensaries and technological advancements.

### Procedure

- a. The Security Officer shall be responsible for coordinating Dispensary's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
- b. The risk analysis shall proceed in the following manner:
  - i. Document Dispensary's current information systems.
    - a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired,

- ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
  - iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
  - iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
  - v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.
  - vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
- e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Dispensary. Consider the following:
- i) Natural threats, e.g., earthquakes, storm damage.
  - ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
  - iii) Human threats
    - a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls

analysis utilizing the standards and implementation specifications to identify vulnerabilities.

- f) Determine and document probability and criticality of identified risks.
  - i) Assign probability level, i.e., likelihood of a security incident involving identified risk.
    - a. "Very Likely" (3) is defined as having a probable chance of occurrence.
    - b. "Likely" (2) is defined as having a significant chance of occurrence.
    - c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
  - ii) Assign criticality level.
    - a. "High" (3) is defined as having a catastrophic impact on the medical dispensary including a significant number of medical records which may have been lost or compromised.
    - b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the dispensary which may have been lost or compromised.
    - c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
  - iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.
- g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those

- i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.
- C. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:
  - i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.
  - ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, Dispensary shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement



HALE MAKAIKE		Policy and Procedure	
Title: Emergency Operations Procedures (EHR outage)		P&P #: IS-2.0	
		Review: Annual	
		Information Technology	

## 15 Emergency Operations Procedures

---

### Purpose

To provide procedures for managing and documenting patient encounters when Electronic Health Record (EHR) and Dispensary Management (PM) systems are unavailable due to planned or unexpected outages.

### Definitions

Electronic Health Record (EHR) – Electronic records of patient encounters in a healthcare delivery setting. An electronic health record typically consists of information including: patient demographics, progress notes, medication history, vital signs and laboratory results.

Dispensary Management (PM) – A dispensary Management System is usually a computer based system used to manage the day-to-day operations of a healthcare dispensary. Tasks typically performed by a PM system include: scheduling appointments, maintaining patient and insurance information, billing functions and generating various reports.

### Procedures

Notification:

### Patient Encounters:

Telephone encounters should be entered onto the paper telephone encounter form and transferred to a nurse for triage.

Out folders should be used as temporary charts.

Paper bills should be used to record patient encounter for billing/tracking purposes. Check-in staff should verify patient's name, date of birth, telephone number, home address, and insurance information as available on the paper; schedule and record all changes on the bill.

If the patient is a walk-in or new patient and demographic information is not available, paper registration forms should be filled out by check-in staff and placed in a temporary chart.

If co-pay information was available on the schedule, or if the patient has a co-pay amount listed on their insurance card, the check-in person should collect as appropriate.

Overhead pages through the telephone system will be used to notify nursing staff when a patient is ready to be taken back.

Paper progress note templates should be used to record usual nurse intake.

Out folder is placed on exam room door as before, using the flag system to notify provider that the patient is ready.

Provider records notes on paper progress notes.

Provider orders are recorded on paper progress notes, while recording the appropriate charges for orders on the paper bill. The out folder is placed on the door and the flag system is used if nurse intervention is needed.

When the provider/nurse is finished with the patient, the provider will complete the encounter form

- Immunizations should be entered into the electronic progress notes.
- Scheduling telephone calls should be returned. A telephone encounter does not need to be entered into the EHR.
- Telephone encounters for all other issues should be entered into the system and routed as appropriate.

Additional Functions:

The Dispensary manager is responsible for maintaining an adequate stock of paper forms in anticipation of system downtime.

Faxes will be evaluated by a nurse for urgency of review by provider.

Items requiring review by a provider will be placed in an out folder on the provider's desk.

All other phone/fax information will be scanned into the patient's record when the EHR system is operational and normal operations have resumed.

HALE MAKAI'IKE (HMI)		Policy and Procedure
Title: Emergency Access “Break the Glass”		P&P #: IS-3.0
		Review: Annual
		Information Technology

## 16 Emergency Access “Break the Glass”

### Policy Summary

The Dispensary has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The Dispensary has a formal, documented emergency access procedure enabling Dispensary workforce members to access the minimum EPHI necessary to effectively and efficiently treat patients in the event of a major medical emergency.

### Purpose

This policy reflects Dispensary commitment to have emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency.

### Definitions

*Medical emergency* means medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

*Electronic protected health information (EPHI)* means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

*Electronic media* means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or

covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

### **Policy**

1. The Dispensary has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The procedure includes:

- Identifying and defining which the Dispensary workforce members authorized to access EPHI during an emergency.
- Identifying and defining manual and automated methods to be used by authorized Dispensary workforce members to access EPHI during a medical emergency.
- Identify and define appropriate logging and auditing that must occur when authorized Dispensary workforce members access EPHI during an emergency.

2. The Dispensary has a formal, documented emergency access procedure enabling Dispensary workforce members to access the minimum EPHI necessary to treat patients in the event of a medical emergency. Such access must be authorized by appropriate Dispensary management or designated personnel.

3. Regular training and awareness on the emergency access procedure is provided to all Dispensary workforce members.

4. All appropriate Dispensary workforce members have access to a current copy of the procedure and an appropriate number of current copies of the procedure should be kept off-site.

### **Scope/Applicability**

This policy is applicable to all divisions and workforce members that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in definitions below.

### **HIPAA Security**

Regulatory Category: Technical Safeguards

#### *Mechanism to Provide Emergency Access to EPHI*

1. This process will bypass formal access procedures and is limited to medical emergencies.
2. The CEO, CIO, Medical Director, or department head<sup>31</sup> may make requests for emergency access in writing.
3. The request should contain:
  - a. The individual being granted the emergency access,
  - b. Job title
  - c. Reason for emergency access
  - d. Date and time granted access
  - e. The name of the individual granting access.
4. The Security Officer<sup>31</sup>, or designated person, records information about emergency users and the emergency access rights assigned to them.
5. The system administrator and Security Officer<sup>31</sup> have created 2 administrator accounts solely for the purpose of emergency access. These accounts should be obviously named, such as breakglass01 and breakglass02 to allow for easy tracking of actions. These accounts and passwords are stored <these accounts need to be located where it would be obvious if they have been used or are missing, as though they were in a fire alarm box which required the glass to be broken to pull the alarm. A location such as in a sealed envelope taped to the side of a monitor in a very conspicuous place such as the nurses' station. Or, they can be locked in an area and require two employees, such as a manager and building security to access. There are a few EHR vendors who have "break glass" access available in their software, but that is not a common ability at this time.><sup>31</sup>
6. The emergency access will be tracked and documented based on capabilities of the EHR. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate.
7. At the conclusion of the event that precipitated the granting of emergency access, the Security Officer ensures the breakglass accounts are disabled, and new ones created in anticipation of the next emergency.
8. Any inappropriate use of emergency access will be treated as a security incident, and may subject an employee to disciplinary action, up to and including termination.
9. Documentation concerning emergency access will be retained and maintained for at least six years from the date of creation.

#### **Note**

HALE MAKAI'IKE (HMI)		Policy and Procedure	
<b>Title: Sanction Policy</b> Security Violations and Disciplinary Action		<b>P&amp;P #:</b> IS-4.0	
		<b>Review:</b> Annual	
		<b>Human Resources</b>	

## 17 Sanction Policy

---

### Policy

It is the policy of the Dispensary that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Dispensary will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The Dispensary will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Dispensary's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, Dispensary's security policies, Directives, and/or any other state or federal regulatory requirements.

### Definitions

*Workforce member* means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

*Sensitive information*, includes, but not limited to, the following:

- Protected Health Information (PHI) Individually identifiable health information that is in any form or

## Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	<ul style="list-style-type: none"><li>• Accessing information that you do not need to know to do your job.</li><li>• Sharing computer access codes (user name &amp; password).</li><li>• Leaving computer unattended while being able to access sensitive information.</li><li>• Disclosing sensitive information with unauthorized persons.</li><li>• Copying sensitive information without authorization.</li><li>• Changing sensitive information without authorization.</li><li>• Discussing sensitive information in a public area or in an area where the public could overhear the conversation.</li><li>• Discussing sensitive information with an unauthorized person.</li><li>• Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.</li></ul>
2	<ul style="list-style-type: none"><li>• Second occurrence of any Level 1 offense (does not have to be the same offense).</li><li>• Unauthorized use or disclosure of sensitive information.</li><li>• Using another person's computer access code (user name &amp; password).</li><li>• Failing/refusing to comply with a remediation</li></ul>



Violation Level	Recommended Disciplinary Action
1	<ul style="list-style-type: none"> <li>• Verbal or written reprimand</li> <li>• Retraining on privacy/security awareness</li> <li>• Retraining on the Dispensary's privacy and security policies</li> <li>• Retraining on the proper use of internal or required forms</li> </ul>
2	<ul style="list-style-type: none"> <li>• Letter of Reprimand*; or suspension</li> <li>• Retraining on privacy/security awareness</li> <li>• Retraining on the Dispensary's privacy and security policies</li> <li>• Retraining on the proper use of internal or required forms</li> </ul>
• 3	<ul style="list-style-type: none"> <li>• Termination of employment or contract</li> <li>• Civil penalties as provided under HIPAA or other applicable Federal/State/Local law</li> <li>• Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law</li> </ul>

•

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Dispensary shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

\*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

#### Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Dispensary.

#### References

U.S. Department of Health and Human Services

EYE CENTER F HAWAII	
Policy and Procedure	
<b>Title: e-Discovery Policy</b> Production and Disclosure of Health Information and Records for e-Discovery	<b>P&amp;P #:</b> IS-5.0
<b>Approval Date:</b>	<b>Review: Annual</b>
<b>Effective Date:</b>	<b>Information Technology</b>

## 18 Discovery Policy: Production and Disclosure

### Policy

It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

### Purpose

The purpose of this policy is to outline the steps in the production and disclosure process for health information and records related to e-discovery for pending litigation.

### Scope

This policy addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures. Health information and records include both paper and electronic data related to relevant patient medical records and enterprise sources.

### Procedure

#### Accurate Patient Identification

Responsible	Action
HIM	For litigation involving an individual's medical records, verify the patient's identity in the master patient index, including demographic information and identifiers including the

Responsible	Action
Litigation Response Team, continued	<ul style="list-style-type: none"> <li>• Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and</li> <li>• Verification that the seal and clerk of the court signature are present and valid</li> </ul> <p>Review of the venue and jurisdiction of the court for the case and verification that the court is located within legal distance/mileage requirements.</p>
HIM	Notify the Litigation Response Team that subpoena has been received and determine if a legal hold is in place. If not, the Litigation Response Team should determine whether a legal hold should be applied.
HIM	<p>If the subpoena requests “any and all records,” HIM and/or Legal Services should work with the judge and/or plaintiff’s attorney to clarify the scope and type of information being requested.</p> <p><i>[Note: The e-discovery process will identify vast volumes of data which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]</i></p>
Litigation Response Team/Legal Services	Provide direction to HIM in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Litigation Response Team/Legal Services	<p>If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to PHI and will need to sign a Business Associate Agreement with this organization.</p> <p>Execute Business Associate Agreement as appropriate.</p>

### Search and Retrieve Process

Responsible	Action
Litigation Response Team	Identify the potential sources of information which may hold potentially relevant information, such as:

Responsible	Action
Litigation Response Team, continued	<ul style="list-style-type: none"> <li>• Text/instant message archives</li> <li>• Removable storage media (e.g., disks, tapes, CDs, DVDs, memory sticks and thumb drives)</li> <li>• Department/office files such as financial records</li> <li>• Personal desk files</li> <li>• Files of administrative personnel in department/office</li> <li>• Files located in department/office staff home</li> <li>• Web site archives</li> </ul>
HIM, Data Owners	<p>Based on direction from the litigation response team on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (patient identifiers, search terms, key words, etc.) and conduct the search process.</p> <p>Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.</p>
IT	<p>Provide assistance to HIM and Data Owners in the search and retrieval process for various systems and data sources.</p>
HIM, Data Owners	<p>Screen or filter the search results, eliminating inappropriate information (e.g., wrong patient, outside the timeframe, not relevant to the proceeding, etc.).</p>
Legal Services	<p>Review the content of the data/data sets found to determine relevancy to the proceeding and identify information that is considered privileged.</p>
Legal Services, HIM, Data Owners	<p>Determine the final list of relevant data/data sets, location, and search methodology.</p>

#### Production of Records/Data

### Charges for Copying and Disclosure

Responsible	Action
HIM, Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
HIM	Invoice requesting parties for allowable charges related to the reproduction of health information and records.
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

### Testing and Sampling

Responsible	Action
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
HIM, Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Litigation Response Team, HIM	Assign a monitor for the outside party during their testing protocols.

### Attorney/Third Party Request to Review Electronic Data

Responsible	Action
Litigation	Determine the procedures for allowing an attorney or third party to review the

Responsible	Action
HIM, Data Owners	Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by a patient or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.

### Responding to Interrogatories, Deposition, Court Procedures

Responsible	Action
Legal Services	Legal Services manages the process for completion of the interrogatories and will coordinate processes related to depositions and testifying in court.
HIM (official record custodian)	HIM may provide information for an interrogatory, be deposed, or testify in court. HIM is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HIM also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system architecture, security dispensaries, source applications, and the good faith operations from a technical infrastructure perspective.
Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The data owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the

**APPROVALS:**

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	

HALE MAKAI'IKE		Policy and Procedure	
<b>Title: e-Discovery Policy</b> Retention, Storage, and Destruction of Paper and Electronic Health Information and Records		<b>P&amp;P #:</b> IS-5.1	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology</b>	

## 19 e-Discovery Policy: Retention

---

### Policy

It is the policy of this organization to maintain and retain enterprise health information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

### Purpose

The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic health information and records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes; and to ensure appropriate availability of inactive records.

### Scope

This policy applies to all enterprise health information and records whether the information is paper based or electronic. It applies to any health record, regardless of whether it is maintained by the Health Information Management Department or by the clinical or ancillary department that created it.

### Definitions

*Data Owners:* Each department or unit that maintains patient health records, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or



## Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
Record Committee	<p><i>[Note: This may be an existing committee, such as the Medical Record Committee, that has membership representing Legal, Compliance, IS/IT, Information Security, HIM, Clinical, and others as appropriate]</i></p> <p>The record committee's role is to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.</p>
HIM	<p>HIM will convene the Record Committee as needed <i>[or at regular intervals]</i> and maintain responsibility for the following:</p> <ul style="list-style-type: none"> <li>• Review, maintain, publish, and distribute retention schedules and records management policies.</li> <li>• Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee.</li> <li>• Serve as point of contact for Records Coordinators.</li> <li>• Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance.</li> <li>• Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services.</li> <li>• Contract for destruction of paper and electronic records and certification thereof.</li> </ul>

Responsible	Action
Records Coordinators	<p>Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following:</p> <ul style="list-style-type: none"> <li>• Transfer records to storage</li> <li>• Identify, control, and maintain records in storage</li> <li>• Retrieve and/or return records from/to storage</li> <li>• Document the destruction of records and the deletion of records from the records inventory</li> <li>• Monitor the records management process</li> </ul> <p>Record coordinators will obtain (if not already trained) and maintain records management skills.</p>
Legal Services	<p>Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters.</p> <p>It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.</p>

#### **Guidelines for Retention of Records/Information and Schedules:**

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated.

E-mail Communication Retention	<p>Depending on content, e-mail messages between clinicians and between patients and clinicians and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format.</p> <p>The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of <i>Messaging Policies</i> that establish disposal schedules for e-mail and manage their e-mail accordingly.</p>
--------------------------------------	---

<p>Development of Records Retention Schedules</p>	<p>Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. <i>[Note: minimum retention schedules are attached to this policy]</i>. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database.</p> <p>Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators.</p> <p>Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section.</p> <p>Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department.</p> <p>Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—typically with e-mail, Microsoft “Office” applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to a “shared drive.” By saving a copy in this manner, IT will create an</p>
---	--

Active/Inactive Records, continued	<p>Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility.</p> <p>Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.</p>
Storage of Inactive Records	<p>All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.</p>
Records Destruction	<p>General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules.</p> <p>Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation.</p> <p>Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include: <i>[Note: specify based on local, state, and federal rule; these could potentially include recycling, shredding, burning, pulping, pulverizing, and magnetizing.]</i><sup>31</sup> A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site</p>

Records Destruction, continued	<p>Disposal of Electronic Media: Electronic storage media, such as CD-ROMs, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include: <i>[Note: specify based on local, state, and federal rules; these could potentially include: burning, shredding, or some other approach which renders the media unusable; degaussing, which uses electro-magnetic fields to erase data; or, preferred for magnetic media when media will not be physically destroyed, "zeroization" programs (a process of writing repeated sequences of ones and zeros over the information)]</i><sup>31</sup>. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed.</p> <p>Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.</p>
--------------------------------	--

**APPROVALS:**

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
<i>[Specify Other Department]</i>			

HALE MAKAI'IKE	
Policy and Procedure	
<b>Title: Reporting and Managing a Privacy Breach Procedure</b>	<b>P&amp;P #:</b> IS-6.0
<b>Approval Date:</b>	<b>Review: Annual</b>
<b>Effective Date:</b>	<b>Information Technology</b>

## 20 Breach Notification Procedures

---

### Purpose

To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HIT HMI), and/or state breach notification purposes.

### Scope

This applies to all employees, volunteers, and other individuals working under contractual agreements with the Dispensary.

### Definitions

State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality, or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

## **Procedure**

### *Reporting a Possible Breach*

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Dispensary will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
  - a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at 808-453-0932.
  - a. Provide the Privacy Officer with as much detail as possible.
  - b. Be responsive to requests for additional information from the Privacy Officer.
  - c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
4. The Privacy Officer, in conjunction with the Dispensary's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

### *Containing the Breach*

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
  - a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
    - i. Stopping the unauthorized dispensary
    - ii. Recovering the records, if possible



- b. The Privacy Officer, in collaboration with the Dispensary's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
  - i. Contractual obligations
  - ii. Legal obligations – the Dispensary's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
  - iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
  - iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
  - v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
  - vi. Number of individuals affected

#### *Notification*

- 1. The Privacy Officer will work with the department(s) involved, the Dispensary's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
- 2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
  - a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
    - i. Notices must be in plain language and include basic information, including:
      - 1. What happened
      - 2. Types of PHI involved
      - 3. Steps individuals should take
      - 4. Steps covered entity is taking
      - 5. Contact Information
    - ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Dispensary in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Dispensary's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the Dispensary will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

#### *Prevention*

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
  - a. If necessary, this will include a security audit of physical, organizational, and technological measures.
  - b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

#### **Compliance and Enforcement**

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Dispensary's Sanction Policy.

#### **Attachments**

# Appendix A – Network Access Request Form

## Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION	
<input type="checkbox"/> New Employee <input type="checkbox"/> New Contractor <input type="checkbox"/> Existing User <span style="float: right;">Today's Date:</span>	
<input type="checkbox"/> Temporary	
First Name:	Last Name: <span style="float: right;">*MI:</span>
Position:	Department: Supervisor:
<input type="checkbox"/> Full-time <input type="checkbox"/> Part-time	Start date or Requested due date: Temporary or Contractor end date, if known:
SECURITY & EMAIL	
New Account: <input type="checkbox"/> Network Account <input type="checkbox"/> Email <input type="checkbox"/> Security/Email similar to what existing user:	
EHR ACCESS	
<input type="checkbox"/> EHR Account	
Roles & Access:	
<input type="checkbox"/> Front Office	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Clinician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Physician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Accounting	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Records Management	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access

## Appendix B – Confidentiality Form

---

### RESPONSIBILITY OF CONFIDENTIALITY

I understand and agree to maintain and safeguard the confidentiality of privileged information Hale Maka'ike, LLC. Further, I understand that any unauthorized use or disclosure of information residing on the Dispensary information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

---

Date

---

Signature

---

Company/Firm

---

Date

---

Signature of Dispensary  
Privacy Officer

## Appendix C – Approved Software

The following list has been approved for use by the Dispensary. All software must be installed and maintained by the appropriate Dispensary personnel.





[illegible]

## Appendix D – Approved Vendors

[illegible]

## Appendix E – Incident Response Tools

---

Tool	Attached Form/Worksheet	Description
Security Incident Report	 Security_Incident-Report-Confidential.doc	Security incident report utilized by the reporting employee or witness to an incident or potential incident.
Security Incident Investigation	 Security_Incident-Investigation-Confident	Security incident investigation report that that allows for further investigation of a potential incident upon receipt of the initial security incident report.
Security Incident Log	 Security_Incident-Log-Confidential.xls	Security incident log to ensure incidents are tracked for further analysis and follow-up.
Security Breach Assessment Tool	 Security_Incident-Breach Assessment-Cor	Privacy breach assessment tool which can assist in determining the severity of a breach.

# Appendix F – Background Check Authorization

---

## AUTHORIZATION AND RELEASE TO OBTAIN INFORMATION

Under the provisions of the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.), the Americans with Disabilities Act, and all applicable federal, state, and local laws, I hereby authorize and permit to obtain a consumer report and/or an investigative consumer report which may include the following:

1. My employment records;
2. Records concerning any driving, criminal history, credit history, civil record, workers' compensation (post-offer only), and drug testing;
3. Verification of my academic and/or professional credentials; and
4. Information and/or copies of documents from any military service records.

I understand that an "investigative consumer report" may include information as to my character, general reputation, personal characteristics, and mode of living, which may be obtained by interviews with individuals with whom I am acquainted or who may have knowledge concerning any such items of information.

I agree that a copy of this authorization has the same effect as an original.

I understand that information obtained in this authorized investigative consumer report and background investigation may result in not being offered a position of employment. I hereby release and hold harmless any person, firm, or entity that discloses information in accordance with this authorization, as well as from liability that might otherwise result from the request for use of and/or disclosure of any or all of the foregoing information except with respect to a violation of the Act. I authorize Hale Maka'ike ("Dispensary") and its designated agent and all associated entities to receive any criminal history information or credit report pertaining to me in the files of any state or local criminal justice agency. I authorize all corporations; companies; former employers; supervisors; credit agencies; educational institutions; law enforcement/ criminal justice agencies; city, state, county and federal courts; state motor vehicle bureaus; and other persons and entities to release information they may have about me to the Dispensary or their designated agent.



My signature below also indicates that I have received a [Summary of Rights](#) in accordance with the Fair Credit Reporting Act.

Date \_\_\_\_\_

Applicant's Signature \_\_\_\_\_

Applicant's Printed Name \_\_\_\_\_

Other Names Used \_\_\_\_\_

Social Security Number \_\_\_\_/\_\_\_\_/\_\_\_\_ Date of Birth \_\_\_\_\_

Driver's License # \_\_\_\_\_ State \_\_\_\_\_

Current Address \_\_\_\_\_

City/Town \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Previous address \_\_\_\_\_

City/Town \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Adapted from <http://www.softHMIinternational.com/SampleReleaseForm.pdf> and  
<http://www.national-employment-screening.com/background-check-release.htm>.

## Appendix G – Change Management Tracking Log

[illegible]

### Merit Criteria – Question 9

In order for our business to be compliant with DOH rule 11-850-81, we intend to implement a laboratory testing process to be set forth in this document to test all of our products in continuation of our FDA / Instrumental Review Board experience and in compliance with the requirements provided by the Department, all to ultimately ensure these products are safe for the consumer.

In order for KMD LLC to be compliant with DOH rule 11-850-82, we intend to implement standard operating procedures (SOPs) and practices (see Appendix 9.1 - **Section 9.3** - Recommended List of Standard Operating Procedures (SOPs) in order for our business to hold the required laboratory certification, independent from all dispensary licensees and employees and all other persons and entities with a financial interest in a dispensary licensee using accredited standards equivalent to the ISO 17025. Our business will also establish SOPs that include chain of custody for samples being transferred to the laboratory for testing. Our business will also meet all of the criteria for laboratory certification in accordance with Chapter 7.

In order for our business to be compliant with DOH rule 11-850-83, we intend to provide all necessary fees and documents required by the department accompanying our application so that we can test our medical marijuana and medical manufactured marijuana

requirements set forth in Chapter 7.

In order for our business to be complaint with DOH rule 11-850-84, we intend to display our certification in a prominent location. We will establish SOPs detailing each step of the procedure including, but not limited to, documentation, sample preparation, reagent preparation, instrument set up and usage, acquisition of data and applicable calculations. We will be in communication with the appointed DOH Department to assure that we are beyond compliant with all accreditation requirements.

In an effort for our business to be complaint with DOH rule 11-850-85, we intend to implement SOPs that reflect ISO standards in testing a statistically representative sample from each batch of medical marijuana or medical manufactured marijuana products and will secure a similar sample from the same batch for verification testing. Our business will test and analyze samples according to SOPs based on scientifically validated methods according to Chapter 7, rule 11-850-85. Our business will also provide a certificate of analysis for each batch of medical marijuana and medical manufactured marijuana products tested for that dispensary and only report on the things for which we are certified to do so (see Section 9.2 – Potency Testing in Appendix 9). In order to remain compliant, procedures for the tests will be based on validated published methods (see Section 9.4 and Section 9.5 of Appendix 9), see table below:

Bacteria, Total Yeast and Mold, Total Coliforms, and Bile-Tolerant Gram Negative Bacteria (Enterobacter)	specific to the species of interest	
E. coli (also called STEC or EHEC), Salmonella spp.	ELISA based screen tests	AOAC and FDA
Aspergillus spp. of mold (Niger, Fumigatus, Flavus)	Morphology and microscopic examination	FDA approved media from the Bacteriological Analytical Manual

All microbial tests conducted will be validated using the FDA approved methods from April 2015 in their document, Guidelines for the Validation of Analytical Methods for the Detection of Microbial Pathogens in Foods and Feeds (see Section 9.1 of Appendix 9). If a batch does not meet acceptance criteria (defined by the Department) for any of the tests above, it will be quarantined and retested. If the retest is still a failure, the batch will be destroyed. We will be prepared to do additional testing at the discretion of the Department. As a business policy, we will create and retain all testing records for a minimum of five years including all provisions in Chapter 7, 11-850-85.

In an effort for our business to be complaint with DOH rule 11-850-86, we intend to follow all rules and regulations set forth in Chapter 7. In case we do not, we are aware of the reasons our laboratory certification may be revoked as set out in section 11-850-86, including

## Merit Criteria – Appendix 9

### **Appendix 9.1 – Microbial Testing Overview**

#### **Scope**

This document will provide general procedure including- time requirements, sample size, storage and disposal- for in house microbial testing of flower and concentrates.

#### **General Process**

Note: SOPs and Methods to be provided at a later date if requested.

- 1) Weigh sample into whirl-pak bag. Record weight.
- 2) Add appropriate amount of diluent
- 3) Massage bag for 1 minute
- 4) Set up serial dilutions
- 5) Plate onto petrifilm or Ecoli/Salmonella tests
- 6) Analyze/Report results after 24-60 hrs
- 7) Store/dispose of extracts and samples

#### **Chemicals Needed**

Note: The local fire department will need to be consulted regarding the storage of chemicals and chemical waste

### **Sample Size Requirements**

<b><u>Sample Type</u></b>	<b><u>Sample Size (minimum)</u></b>
Flower, bud, trim	1 gram
Concentrates (extract oil, wax, etc.)	1 gram

### **Sample Time Requirements**

<b><u>Process</u></b>	<b><u>Time requirements</u></b>
Sample Prep	5 minutes (per sample)
Sample Dilutions	10 minutes (per sample)
Sample Plating	3 minutes (per sample)
Sample run time	24-60 hours (per sample) can do up to 350
Sample Analysis Time	5 minutes (per sample)

### **Sample Capacity**

<b><u>Process</u></b>	<b><u>Capacity</u></b>
Sample Preparation	25-40 samples per day per person
Incubator Capacity	480 petrifilms per day (including QCs) 50 100 Ecoli and Salmonella tests per day

## **Disposal**

This may depend on final State regulations but we have provided a suggested protocol as noted Merit Question Response 11.

## **Testing Frequency**

This may depend on final regulations, but recommendations are as follows:

- 2% of every strain of flower harvested
- 2% of every batch of oil produced

## **9.2 – Potency Testing**

### **Scope**

This document will provide general procedure including- time requirements, sample size, storage and disposal- for in house potency testing of flower and concentrates.

### **General Process**

Note: SOPs and Methods to be provided at a later date if requested.

- 8) Weigh sample into conical vial. Record weight.
- 9) Add appropriate amount of extraction solvent
- 10) Sonicate
- 11) Dilute with extraction solvent (to make sure extract is within quantifiable range)



- 1) Methanol
- 2) Chloroform
- 3) Formic Acid
- 4) Ammonium Formate
- 5) Acetonitrile
- 6) HPLC grade Water
- 7) Reference Standards for each cannabinoid to be analyzed

#### **Sample Size Requirements**

<b><u>Sample Type</u></b>	<b><u>Sample Size (minimum)</u></b>
Flower, bud, trim	0.200 grams
Concentrates (extract oil, wax, etc.)	0.0500 grams

#### **Sample Time Requirements**

<b><u>Process</u></b>	<b><u>Time requirements</u></b>
Sample Weighing	1 minute (per sample)
Sample Extraction	30 minutes per batch of samples (~25)
Sample Dilution	1 minute (per sample)

### **Sample Capacity**

<b><u>Process</u></b>	<b><u>Capacity</u></b>
Sample Preparation (Extraction)	100 samples per day per person
UPLC/PDA Sample Capacity	288 samples per day (including QCs)

### **Storage**

<b><u>Sample Type</u></b>	<b><u>Storage Time</u></b>
Sample (flower, concentrate, etc.)	3 months
Sample extract	1 week

### **Disposal**

This may depend on final State regulations but we have provided a suggested protocol as noted Merit Question Response 11.

### **Testing Frequency**

This may depend on final regulations, but recommendations are as follows:

- Sample from each 10 pounds of harvest (~25 samples per 250 lbs. of the same strain)
- A sample from each production batch that will be given to a patient

## **9.3 – Recommended List of Standard Operating Procedures (SOPs)**

- 4) Plating-Coliform/Enterobacter
- 5) Cell Count
- 6) Ecoli Testing
- 7) Salmonella spp. Testing
- 8) Aspergillus spp. Testing
- 9) Mycotoxin Testing
- 10) Autoclave Operation and Maintenance
- 11) Biohazard Waste
- 12) Documentation of experiments and results
- 13) Media Preparation
- 14) Organism Maintenance
- 15) Laboratory Notebook Procedure
- 16) Sample Receipt, Handling, Storage and Disposal
- 17) Training Procedure
- 18) Method Validation Procedure
- 19) Potency Extraction
- 20) Potency Analysis

#### 9.4 – Validated Procedures

<b>Test Type</b>	<b>Equipment</b>	<b>Validation Based On</b>
<b>Chemical Profile</b>	<b>UPLC(HPLC)/UV Detector</b>	<b>FDA/GLP Guidelines</b>
<b>Heavy Metals</b>	<b>ICP-MS</b>	<b>EPA</b>
<b>Pesticides</b>	<b>LC-MS/MS</b>	<b>EPA</b>
<b>Solvents</b>	<b>GC-FID</b>	<b>US Pharmacopeia Chapter 467</b>
<b>Visible foreign and extraneous material</b>	<b>Microscope or visual</b>	<b>FDA</b>
<b>Moisture Content</b>	<b>Oven</b>	<b>ISO Method</b>
<b>Total Viable Aerobic Bacteria, Total Yeast and Mold, Total Coliforms, and Bile-Tolerant Gram Negative Bacteria (Enterobacter)</b>	<b>3M petrifilm plates specific to the species of interest</b>	<b>AOAC</b>
<b>E. coli (also called STEC or EHEC), Salmonella spp.</b>	<b>ELISA based screen tests</b>	<b>AOAC and FDA</b>
<b>Aspergillus spp. of mold (Niger,</b>	<b>Morphology and</b>	<b>FDA approved</b>

Thomas Scientific for this as I have had great experiences with their company and customer service in the past. Upon initial lab set up, they will also provide a pretty large discount (the last lab I did this with received roughly a 30% discount overall). We have no affiliation with them, just great experiences so we would like to recommend them. We have included current prices for these items as well to give you a general idea, however, these prices may change.

### **Potency/Chemistry**

For the big ticket items, i.e., purchasing most of the equipment used will be a more cost effective approach. I will see what is out there and request quotes. Please note that quotes usually take about a week to finalize with used equipment. It will also take rough 3-4 weeks to deliver. I would like to hold off on ordering or getting quotes for these items until Costa Farms is ready to purchase as inventory is constantly changing. For the equipment lists, I have quoted new prices to give a general sense of the upper end of cost.

### **UPLC recommendation**

Although you have other options, I would still recommend using the Water UPLC/PDA as this system is the most reliable if it is not consistently being run on a daily basis. Waters has also provided very good customer service in my experience. The method that we will use on this can be validated based on FDA guidelines which are some of the strictest for analytical assays. I

tools used in qPCR are not only expensive but require an experienced hand in processing samples. For the time being, Salmonella species and STEC Ecoli are the only tests that can be done on PCR with accuracy. The maintenance required on a regular basis can also decrease cost effectiveness if there are periods where you will not be testing samples.

I have suggested assays for STEC Ecoli and Salmonella that are protein type assays. They require the organism to be alive and do not require expensive instruments or an experienced hand to process or analyze results. I have also suggested using pre-made rapid plating tests that reduce prep time and give accurate results faster than regular plating methods. These pre-made plates are also easy for colony counting and easy to use.

For these reasons, I chose different assays that eliminate these issues for your testing requirements. All are accredited by the AOAC (**association of analytical communities**) Which requires rigorous validation studies across multiple labs.

### General Lab Equipment

Category	Item	Supplier	Part number	Cost	Unit	Quantity	Total Cost
Personal Protective Equipment	Lab coats	Thomas Scientific	12321894	\$ 33.34	Each	10	\$ 333.40
	Lab coat hooks	Amazon		Command hooks will work			
	Wall mount for gloves Acrylic	Thomas Scientific	1222K05	\$ 70.95	Each	1	\$ 70.95
	Gloves Nitrile Small	Thomas Scientific	5761R17	\$ 187.00	Case (1000)	1	\$ 187.00
	Gloves Nitrile Medium	Thomas Scientific	5761R21	\$ 187.00	Case (1000)	1	\$ 187.00
	Gloves Nitrile Large	Thomas Scientific	5761R27	\$ 187.00	Case (1000)	1	\$ 187.00
	Gloves Nitrile Extra Large	Thomas Scientific	5761R46	\$ 187.00	Case (1000)	1	\$ 187.00
	Wall mount for glasses	Thomas Scientific	1215X12	\$ 172.00	Each	1	\$ 172.00
	Safety Glasses	Thomas Scientific	1199035	\$ 2.53	Each	10	\$ 25.30
	Ear Plugs	Thomas Scientific	1216269	\$ 47.30	200	1	\$ 47.30
Safety/ Medical	Emergency Eye Wash	Thomas Scientific	1224B27	\$ 52.55	3	1	\$ 52.55
	Chemical Spill Kit	Thomas Scientific	8238805	\$ 186.76	1	1	\$ 186.76
	First Aid Kit	Thomas Scientific	1233196	\$ 163.45	1	1	\$ 163.45
	Fire Extinguisher						\$ -
	Emergency Shower						\$ -
Glassware	Media Bottles 100ml	Thomas Scientific	1395-100	\$ 93.17	Case (10)	1	\$ 93.17
	Media Bottles 500ml	Thomas Scientific	1395-500	\$ 123.66	Case (10)	1	\$ 123.66
	Media Bottles 1000ml	Thomas Scientific	1395-1000	\$ 151.84	Case (10)	1	\$ 151.84
	Media Bottles 2000ml	Thomas Scientific	1395-2000	\$ 399.89	Case (10)	1	\$ 399.89
	Beaker 100ml	Thomas Scientific	1531H76	\$ 191.26	Pack (12)	1	\$ 191.26
	Beaker 500ml	Thomas Scientific					\$ -
	Beaker 1000ml	Thomas Scientific	1531P51	\$ 86.28	Pack (6)	1	\$ 86.28
	Erlenmeyer Flask 125ml	Thomas Scientific	4907F23	\$ 98.16	Pack (12)	1	\$ 98.16
	Erlenmeyer Flask 500ml	Thomas Scientific	4907F35	\$ 55.84	Pack(6)	1	\$ 55.84
	Erlenmeyer Flask 1000ml	Thomas Scientific	4907F41	\$ 94.23	Pack(6)	1	\$ 94.23
	Volumetric Flask 10ml	Thomas Scientific	0319B48	\$ 285.38	12	1	\$ 285.38
	Volumetric Flask 50ml	Thomas Scientific	0319U75	\$ 36.67	1	5	\$ 183.35
	Volumetric Flask 100ml	Thomas Scientific	0319B45	\$ 330.52	12	1	\$ 330.52
	Volumetric Flask 500ml	Thomas Scientific	0319W81	\$ 60.50	1	3	\$ 181.50
	Volumetric Flask 1000ml	Thomas Scientific	0319B41	\$ 72.81	1	3	\$ 218.43
	Graduated Cylinder 50ml	Thomas Scientific	3557B73	\$ 21.34	Each	3	\$ 64.02
	Graduated Cylinder 100ml	Thomas Scientific	3557B77	\$ 25.11	Each	3	\$ 75.33
	Graduated Cylinder 500ml	Thomas Scientific	3557B85	\$ 56.84	Each	3	\$ 170.52
	Graduated Cylinder 1000ml	Thomas Scientific	3557B89	\$ 70.69	Each	3	\$ 212.07
	Graduated Cylinder 2000ml	Thomas Scientific	3557B93	\$ 115.11	Each	3	\$ 345.33
General	Kimwipes Small (4.4x6.4)	Thomas Scientific	2904F24	\$ 8.74	Box (280)	5	\$ 43.70
	Kimwipes Large (11.8x11.8)	Thomas Scientific	2904F39	\$ 9.59	Box(196)	5	\$ 47.95
	Parafilm	Thomas Scientific	1222K01	\$ 73.48	4"x250ft	2	\$ 146.96
	Sharpie Markers	Amazon					\$ -
	Label Tape	Thomas Scientific	1209K22	\$ 49.55	Case (12) 500"	1	\$ 49.55
	Spatulas Various	Thomas Scientific	1232X12	\$ 82.85	7 assorted	3	\$ 248.55
	Spatulas Scoop	Thomas Scientific	1195R87	\$ 32.03	Pack(12)	1	\$ 32.03
	Bench/Mixer Vortexer	Thomas Scientific	1227U58	\$ 235.00	Each	2	\$ 470.00
	Timer	Thomas Scientific	9371W52	\$ 32.48	Each	2	\$ 64.96
	Lab Notebooks	Scientific Notebook Company	2001HC	\$ 19.00	Each	5	\$ 95.00
	Wash Bottles	Thomas Scientific	1186Z39	\$ 28.60	Pack (5)	1	\$ 28.60
	Thermometer	Thomas Scientific	9313A86	\$ 25.14	Each	4	\$ 100.56
	Tweezers	Thomas Scientific	1199R87	\$ 9.49	Each	4	\$ 37.96
	Lab benches						\$ -
	Chairs	Uline	H-1375	\$ 209.00	Each	2	\$ 418.00
	MSDS Safety Sign						\$ -
	Fire Extinguisher Safety sign	Thomas Scientific	1190R19	\$ 10.60	Each	2	\$ 21.20
	3 bay sink						\$ -
	Eye Wash Safety Sign	Thomas Scientific	1215U10	\$ 13.56	Each	1	\$ 13.56

### Microbial Testing Lab Equipment

Category	Item	Supplier	Part number	Cost	Unit	Quantity	Total Cost
<b>General</b>	Cell counter (hemocytometer)	Amazon	634-6310	\$ 160.00	Each	2	\$ 320.00
	Balance to 0.01g	Thomas Scientific	1218V30	\$ 3,706.00	Each	1	\$ 3,706.00
	Pipettes p10,p200,p1000	VWR	89133-288	\$ 1,178.31	set	1	\$ 1,178.31
	Pipette tips for above						
<b>Plating</b>	Incubator 35	Thomas Scientific	1187Q10	\$ 3,549.00	Each	1	\$ 3,549.00
	Incubator 25	Thomas Scientific	1187Q10	\$ 3,549.00	Each	1	\$ 3,549.00
	4 deg fridge for organisms *	Thomas Scientific	8050H12	\$ 2,181.36	Each	1	\$ 2,181.36
	Autoclave	Thomas Scientific	1213N94	\$ 7,886.00	Each	1	\$ 7,886.00
	Colony counter with backlight	Thomas Scientific	1199K33/1199K34	\$ 2,413.30	Each	1	\$ 2,413.30
	Pipetteman	Thomas Scientific	1203G40	\$ 144.22	Each	1	\$ 144.22
	Magnetic stir/heat blocks	Thomas Scientific	8613L22	\$ 952.20	Each	2	\$ 1,904.40
	BSL II hood (Laminar Flow)	Thomas Scientific	1204H29	\$ 17,445.00	Each	1	\$ 17,445.00
<b>Mycotoxins</b>	Microscope (10x)	Thomas Scientific	1195A23	\$ 574.00	Each	1	\$ 574.00
	8 channel pipettor	Thomas Scientific	1221U36	\$464.40	Each	1	\$ 464.40
	Microwell reader	Romer	EQ01E4700	2,500.00	each	1	\$ 2,500.00
	Magic Bullet small silver with cups	Amazon		39.99	each	1	\$ 39.99

\*Should be small stand alone fridge

Note: Quantities are rough estimates and will vary based on the size of the lab and lab staff



### Microbial Testing Lab Consumables

Category	Item	Supplier	Part number	Cost	Unit	Quantity	Total Cost
General	Whirl Pak Bags	Thomas Scientific	1303N08	\$ 187.05	250/bx	1	\$ 187.05
	Buttered Peptone Water	Thomas Scientific	C941F21	\$ 53.63	500g	1	\$ 53.63
	Butterfield's Buffer	Thomas Scientific	1750070	\$ 108.84	72/pl	1	\$ 108.84
	2ml pipette tips	Thomas Scientific	1195088	\$ 46.35	768/pl	1	\$ 46.35
	Salmonella typical	Microbiologies	0901P	\$ 150.00	2 sticks	1	\$ 150.00
	Salmonella atypical	Microbiologies	01054P	\$ 150.00	2 sticks	1	\$ 150.00
	STEC E.coli	Microbiologies	01204P	\$ 150.00	2 sticks	1	\$ 150.00
	E.coli	Microbiologies	0495P	\$ 150.00	2 sticks	1	\$ 150.00
	Yeast	Microbiologies	0332P	\$ 150.00	2 sticks	1	\$ 150.00
	Coliform	Microbiologies	0839P	\$ 150.00	2 sticks	1	\$ 150.00
	Mold	Microbiologies	0178P	\$ 150.00	2 sticks	1	\$ 150.00
	Dextrose	Thomas Scientific	C979Y90	\$ 115.20	500g	1	\$ 115.20
	Agar	Thomas Scientific	1773490	\$ 177.13	500g	1	\$ 177.13
	Ferrie Ammonium Citrate	Thomas Scientific	C993Z36	\$ 38.24	100g	1	\$ 38.24
	Peptone	Thomas Scientific	C997A05	\$ 75.00	500g	1	\$ 75.00
	Gentamycin	Thomas Scientific	C000R58	\$ 136.10	5g	1	\$ 136.10
Reusable Supplies	Star bars	Thomas Scientific	1207P99	\$ 10.15	Each	4	\$ 40.60
	Thermometer	Thomas Scientific	9313A86	\$ 25.14	Each	4	\$ 100.56
	Bottle sterilizer (alcohol lamp)	Thomas Scientific	2077G85	\$ 76.33	Each	1	\$ 76.33
	plate spreader for RYM	Carolina	824105	\$ 8.50	Each	5	\$ 42.50
	Plate spreader for all other	Carolina	824100	\$ 7.50		5	\$ 37.50
Organism Detection Supplies	Rapid salmonella test	Romer Labs	7000190	\$ 882.00	100 tests	1	\$ 882.00
	ImmunoCard Stat, EHEC,						
	for the detection of Shiga toxins	Hardy Diagnostics	751630	\$ 1,300.00	30 tests	1	\$ 1,300.00
	RYM Petrifilm	Thomas Scientific	1185X02	\$ 137.71	50/bx	1	\$ 137.71
	Rapid Aerobic Petrifilm	Thomas Scientific	1185X20	\$ 96.92	50/cs	1	\$ 96.92
Mycotoxin Detection Supplies	*Enteroc/coliform Petrifilm	Thomas Scientific	1185X10	\$ 117.94	50/cs	1	\$ 117.94
	Methanol ACS Grade	Thomas Scientific	C389182	\$ 593.00	4x4L	1	\$ 593.00
	Whatman 1 paper	Thomas Scientific	4712945	\$30.92	100/pl	1	\$30.92
	reagent boat	Thomas Scientific	1278R19	\$115.00	200/box	1	\$115.00
	AgraQuant® Total Aflatoxin assay	Romer Labs	CORAO1000	310	96 well	1	\$310.00
	AgraQuant® Ochratoxin Assay	Romer Labs	CORAO2000	310	96 well	1	\$310.00
	Mycoscep112 column	Romer Labs	COCAF2112	135	25/pl	1	\$135.00
	Filter funnel	Thomas Scientific	S207W41	\$65.2	2	1	\$65.2

also noted in Chemistry can borrow

Note: Quantities are rough estimates and will vary based on the size of the lab and lab staff

## Merit Criteria - Question 10

KMD LLC has solicited proposals from several packaging companies to service our needs for both shipping from our production center to our retail dispensing location as well as point of sale transactions to our patients. We will make our final selection of this packaging partner based upon their ability to deliver upon the requirements set forth within Section 329D-11, HRS and other variables including cost, reputation and best practices with regard to medical marijuana and consumer safety prior to the retail dispensary becoming operational.

Prior to shipping any medical marijuana-related products from production to retail, KMD LLC will have appropriately sized shipping containers on-site, requiring the use of tamper evident lids, constructed out of opaque material, sealed with tamper evident tape and signed by no less than two managers on duty. The packaging manager will be responsible for sealing and initialing the package with tamper evident tape. The shipment will be placed on a shipping pallet and loaded for transport.

All products being shipped from the production center to the retail location will have a unique label generated by BioTrackTHC software. All labeling will be generated from BioTrackTHC, ensuring the product history is easily traceable. Included in this label will be: 1)

All packaging and labeling at the dispensary will comply with Section 329D-11, HRS, at a minimum, for the sale of the product to the patient. The packaging for marijuana will be placed in ASTM child-resistant, opaque bags or containers and will contain no more than the patient's allowable purchase amount which will be verified by the inventory tracking system. The packaging for medical manufactured marijuana products will be pre-packaged in ASTM child-resistant, opaque packaging and contain no more than 100 milligrams of THC per package. In addition, all medical manufactured marijuana product packaging will be in accordance with Section 329D-9, HRS (see Appendix 10 - Section 10.3 - Packaging and Labeling Plan - Manufactured Products).

BioTrackTHC will automatically print the container-client specific label upon completion of a sale to a qualifying patient. The name and address of the recipient, the quantity delivered, and the product name, potency, batch number, and lot number of the product can all be recorded for each distribution. For a full list of fields currently integrated into BioTrackTHC, please see Appendix 10.1 - BioTrackTHC Label Fields.

BioTrackTHC will also assist us in tracking chain of custody from plant clone to point of sale, in accordance with Hawaii Administrative Rules, Subchapter 5, Section 11-850-61. At the



## **Merit Criteria - Appendix 10**

### **10.1 - BioTrackTHC Label Fields (Current as of 1/20/16)**

Custom Text Fields, Images, Lines, Additives, Barcode, Batch #, Custom Batch #, Customer Medical Marijuana ID #, Customer Name, Date, Date and Time, Employee Name, Employee License #, Grow (Production) License #, Harvest Date, Inventory Grade, License #, MITS ID, Package Date, Package Weight, Plant Birthdate, Product Expiration, Product Ingredients, Product Name, Strain, Strain Type, Testing Date, Testing Lab, Usable Weight, Weight, Test Results (including: CBC, CBD, CBD-A, CBG, CBN, D8-THC, D9-THC, D9-THC-A, H2O, Heavy Metals, Mold, Mildew, Total THC, Total Cannabinoids)

### **10.2 – Sample Exit Bag**





Courtesy of FunkSac™

### 10.3 Packaging and Labeling Plan - Manufactured Products

Labeling requirements on content and format for medical marijuana will conform to state mandated regulations and the FDA's CFR Title 21, part 201. Medical marijuana infused products will be individually packaged and labeled immediately at the point of preparation. All marijuana infused products that are shipped to a dispensary from the cultivation center will be in ASTM certified child resistant packaging and will conform to the requirements Title 16 CFR 1700 of the

container will not contain more than 100 milligrams total THC. Each packaged and labeled product will bear a clear warning to keep the package and its contents away from children. A SAFETY NOTICE on the label will include the dosing information along with the Poison Control Center emergency telephone number in case of accidental ingestion or adverse effect.

Medical marijuana and medical marijuana extract utilized in the creation of all medical marijuana infused products will be lab tested for cannabinoid profile, microbiological contaminants, mycotoxins, pesticide active ingredients, residual solvent, and active ingredient analysis. The accurate cannabinoid profile information will be utilized in the production formulations and standard operating procedures for marijuana infused product production to ensure accurate cannabinoid dosing and labeling. Marijuana Infused Products will be assigned a Production Batch Number that utilizes verified and accurate lab test results. This system allows the marijuana infused product to be directly traced to the marijuana plant(s) from which the cannabinoid profiles originate. This process allows for accurate test result information to be displayed on the marijuana infused product label as well as being integral to seed-to-sale traceability.

Incorporated into the product label will be a blank area. A separate batch-label sticker will be created for each unit of product that will be affixed to the product within this designated

Products will contain non-cannabis ingredients. All non-cannabis ingredients will be listed in a weighted format per FDA guidance. The most dominant ingredient will be listed first and the least dominant will be listed last. This information will be printed within a designated area on the product label and will be clearly legible showing non-cannabis ingredients contained within an outlined box.

Product labels will be completely wrapped in opaque 4mm shrink-wrapped labels. The labels of medical marijuana infused products will be designed with black lettering with no pictures or graphics. Information represented on the labels will include but not be limited to the following information:

PRODUCT LABEL CONTENT:

1. The name of the Production Center
2. Instructions for use
3. An inventory tracking barcode for use by tracking software that will match the product with a producer batch and lot number to facilitate any warnings or recalls the Department or producer deems appropriate.
4. Type of extraction method used including solvents, gases or other chemicals or compounds used to produce the marijuana product.



8. The statement “This product may be unlawful outside of the State of Hawaii and is unlawful to possess or use under federal law.”
9. The statement “This product has intoxicating effects and may be habit forming.”
10. The statement “Smoking is hazardous to your health.”
11. The statement “There may be health risks associated with consumption of this product.”
12. The statement “This product is not recommended for use by women who are pregnant or breastfeeding.”
13. The statement “Marijuana can impair concentration, coordination and judgement. Do not operate a vehicle or machinery under the influence of this drug.”
14. The statement “When eaten or swallowed, the effects of this drug may be delayed by two or more hours.”
15. The statement “This product is not for resale or transfer to another person”.
16. The identification of the independent testing laboratory.

PRODUCTION BATCH STICKER UNIQUE TO EACH BATCH:

1. Dispensary License Number
2. The date of packaging and "use by" date
3. Production Batch Number

- CBD
- CBDA
- Total CBD

**Chain of Custody**

Medical marijuana product production begins with lab tested and approved marijuana extract. All product production staff will be trained in company SOPs (see Standard Operating Procedures).

An employee of the Extraction Area will deliver medical marijuana extract from the Extraction Area into the Production Area. All medical marijuana extract moved into the Production Area will be documented and inventoried by an employee of the Production Area. The chain of custody of the marijuana extract from extraction area to the production area will be documented in the inventory tracking software. A designated production employee will conduct daily inventory of all medical marijuana extract and products within the production area at the beginning and ending of every day.

All non-marijuana products will be inventoried and inspected before being brought into the Production Area and will be stored in a separate storage area or in climate-controlled coolers or freezers on stainless steel racks. Layout of the Production Area will be segregated into 4 main

Medical marijuana product production will be under the supervision of a certified food sanitation manager. Staff employed within the production area will have a recognized food handler certification and will manage, prepare, package, and label all medical marijuana products for distribution to a dispensing facility. The Production and Extraction Areas will be considered Limited Access Areas with entry permitted only to employees validated to work in those areas.


Medical marijuana products will be non-hazardous and certified shelf-stable. Approved non-marijuana ingredients will be received and stored accordingly. The lot and batch numbers of all approved non-marijuana ingredients will be logged and recorded to assist in the event of a product recall. Employee and product health and security will be a priority of the production area.

Inventory of all medical marijuana products will be performed and recorded throughout each day. More than one employee including a manager will verify the inventory results. All staff will be trained in internal Standard Operating Procedures (SOP) of the production areas. A designated Compliance Officer will be on site at all times of production to ensure compliance with all state and local laws and to ensure accurate medical marijuana inventory tracking utilizing inventory tracking software. All medical marijuana products will be secured at all times

### 10.3.1 Sample Label Image

## SAMPLE PRODUCT LABEL

\*\*\* An inventory tracking barcode for use by tracking software that will match the product with a producer batch and lot number to facilitate any warnings or recalls the Department or producer deems appropriate.

<b>THIS PRODUCT IS NOT RECOMMENDED FOR USE BY WOMEN WHO ARE PREGNANT OR BREASTFEEDING.</b>	<b>THIS PRODUCT HAS INTOXICATING EFFECTS AND MAY BE HABIT FORMING.</b>	<b>INDEPENDENT TESTING LABORATORY IDENTIFICATION</b>
There may be health risks associated with consumption of this product.	FOR MEDICAL USE ONLY SMOKING IS HAZARDOUS TO YOUR HEALTH.	<i>When eaten or swallowed, the effects of this drug may be delayed by two or more hours.</i>
This product is not for resale or transfer to another person.	<div>PRODUCT</div>	Marijuana can impair concentration, coordination and judgment. Do not operate a vehicle or machinery under the influence of this drug.
Net Wt:		Contains no more than 10mg THC for one dose, no more than 100mg THC in container.
 0 123456 789012	NAME OF PRODUCTION CENTER	DATE OF MANUFACTURE:
INSTRUCTIONS FOR USE: Type of extraction method used including solvents, gases or other chemicals or compounds used to produce the marijuana product. All ingredients of the item, including any colors, artificial flavors and preservatives, listed in descending order by predominance of weight shown with common or usual names.		
ALLERGEN LABELING: This product may be unlawful outside of the State of Hawaii and is unlawful to possess or use under federal law.		
<div>Product Name _____ Product Weight _____ Product Lot Number _____ Product Expiration Date _____ For product use only. Do not use if any of these fields is blank.</div>		

\*\*\* Production Batch Sticker  
Unique To Each Batch

### Merit Criteria - Question 11

Upon award of a Hawaii dispensary license and prior to handling of any marijuana, KMD LLC shall apply to the department of public safety narcotics enforcement division (NED) and obtain a certificate to possess and handle marijuana and manufactured marijuana products. Ultimately, KMD LLC intends to destroy or dispose of unused, unsold, contaminated, expired, or mishandled marijuana or manufactured marijuana products by a means prescribed by the department of health or the department of public safety narcotics enforcement division administrator in accordance with Hawaii Administrative Rules, Subchapter 3, Section 11-850-43, Disposal or Destruction. Upon approval by the NED, KMD LLC will establish written policies and procedures to be followed by all employees in regard to destruction and disposal of all unused, unsold, contaminated, expired, or mishandled marijuana and manufactured marijuana products as part of it's standard operating procedures.

To ensure the secure destruction and disposal of marijuana and manufactured marijuana products, KMD LLC intends to implement a robust disposal protocol at our production center(s). These locations will serve as the primary point of destruction and disposal for waste products, typically in the form of stalk, stems, unrooted clones, dry and dead leaves, topped, pruned and de-fanned plant matter, generated from production and cultivation of marijuana, manufacturing of

tracking identification issued by the tracking system, the identity of the person transporting the marijuana or manufactured marijuana products, and the make, model, and license number of the vehicle being used for transport.

All forthcoming destruction and disposal procedures will be performed by an approved full time staff member in the presence of a manager to ensure double verification of the process. In addition, security systems will monitor the process in its entirety, limiting the potential for diversion within the interior or exterior of the production center.

All wasted material will be deemed not only unusable, but also unrecognizable prior to leaving KMD LLC facilities in accordance with the following procedures:

**Procedure 1:** KMD LLC will assure proper waste inventory tracking;

- KMD LLC will maintain accurate and comprehensive records regarding any waste material produced through the trimming or pruning of a medical marijuana plant prior to harvest, which must include weighing and documenting all waste. Records of waste produced prior to harvest will be maintained on the premises of KMD LLC. Waste produced prior or subsequent to harvest will be disposed of in accordance with this policy and made unusable and unrecognizable.
- KMD LLC will ensure its marijuana waste materials are identified, weighed and tracked

- KMD LLC will maintain accurate and comprehensive records regarding waste material that accounts for, reconciles, and evidences all waste activity related to the disposal of medical marijuana and manufactured marijuana products and will be made available to the department or law enforcement upon request.

**Procedure 2:** Grinding and incorporating the cultivated marijuana waste products via an electronic grinder, chipper, shredder or mulcher; including unviable plants, plant stalks, plant stems, and plant fan leaves, with non-consumable, solid wastes listed below such that the resulting mixture is at least fifty percent non-marijuana waste including:

- Paper waste;
- Cardboard waste;
- Spent soil waste (dirt);
- Grease or other compostable oil waste;
- Bokashi, or other compost activators; or
- Other wastes approved by the NED that will render all medical marijuana and manufactured marijuana product waste unusable and unrecognizable.
- All wasted marijuana and manufactured products to be destroyed shall be mixed so that at least fifty percent of the total mixture is composed of items listed above and treated with

- KMD LLC will assure that any waste receptacle is secured inside the locked enclosure until it is scheduled to be picked up by a third-party authorized by the NED.

*Or*, the resultant sanitized mixture will be placed within a compost dumpster destined for a sanitary landfill application on the exterior of the production center. KMD LLC will work with the DOH and NED to determine the preferred final methodology.

**Procedure 4:** KMD LLC will maintain a contract with a Hawaii-licensed waste disposal company authorized by the department or NED in the handling of marijuana waste disposal.

- KMD LLC will designate a manager to monitor the current contract to be sure it is current and on record for inspection by the department as necessary.
- KMD LLC manager will meet the third-party waste disposal agent and validate their authority to remove marijuana waste that has been rendered unusable and unrecognizable.
- KMD LLC manager will document the waste pick up in the inventory tracking system.
- Records will be maintained on premise for a minimum of six years.
- KMD LLC will maintain an independent log of such disposal that will be kept at the production center for inspection by department officials or law enforcement as required.

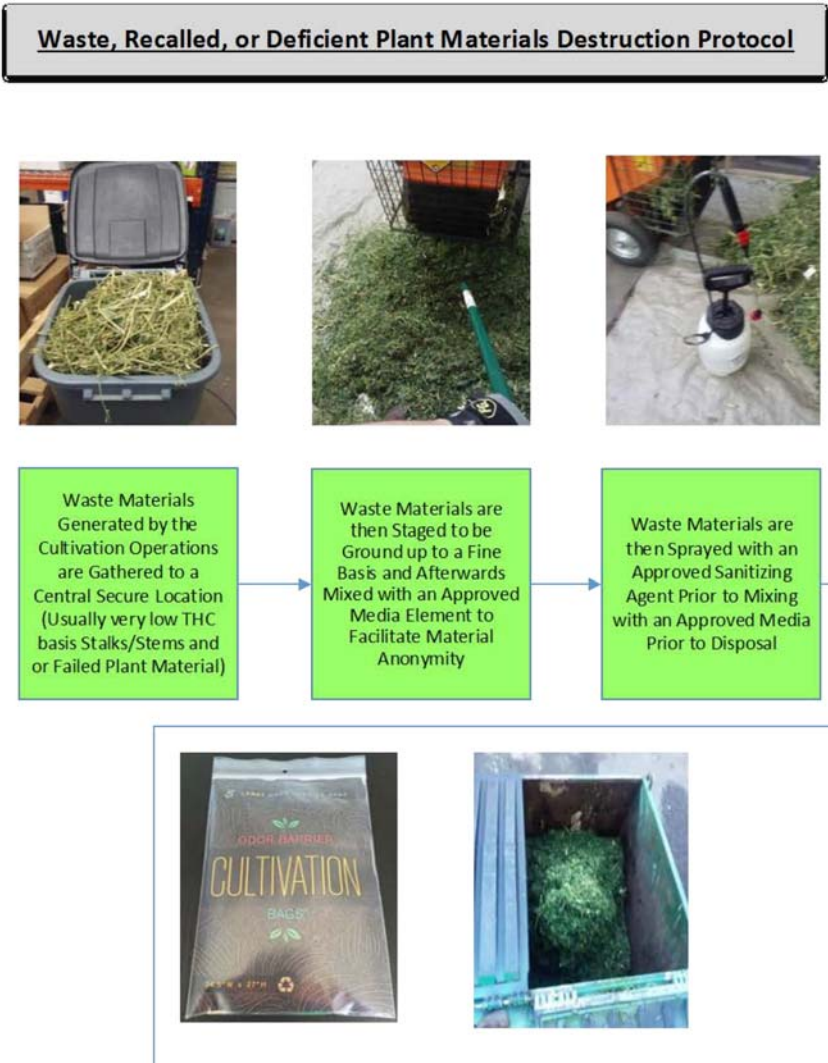
For a summary flowchart and representative photos please see Appendix 11 - Section 11.1 - Destruction and Disposal Process Flow and Photos.



inventory audits) and external factors (such as theft and seizure by law enforcement). Data related to disposal information may include but is not limited to: the amount disposed, reasons for disposal, day/time of disposal, identity of the employee(s) conducting the disposal, and manner of disposal in addition to all product-related data such as inventory classification.

Merit Criteria Appendix 11

11.1 – Destruction and Disposal Process Flow & Photos (File Photo Similar)



### **11.2 – Disposal of Manufactured Marijuana Product**

If it is determined that a product or substance at any stage within the manufacturing process containing marijuana does not meet quality standards, is outdated, damaged, deteriorated, misbranded, adulterated or whose container or package has been improperly or accidentally opened, it may be determined to be disposed of in accordance with Company waste-disposal policies and procedures and regulatory requirements.

The SOP will include:

1. Segregation - Location within facility designated for waste storage. Access will be limited to authorized personnel.
2. Disposal by authorized personnel - Supervisory approval will be required on all medical-cannabis waste and products designated for disposal. These segregated inventories are clearly identified with a label that includes signature of supervisory personnel.
3. Render substance unusable - Clear description of waste-handling procedures including protocols for rendering substance unusable prior to disposal. This will include mixing waste with non-consumable solid-wastes such that the resulting mixture is at least 50-percent non-cannabis waste.
4. Procedures performed in view of video surveillance security equipment with multiple

This production facility shall not dispose of marijuana waste in an unsecured waste receptacle not in possession and control of the production facility within the waste disposal area. Only authorized employees will have the access level to destroy product and ensure the destroyed weight and the reason for destruction are recorded in Inventory Tracking Software. Inventory Tracking Software can generate reports on the number and/or weight of destroyed material at any point in the process. Every action will be recorded with a date/timestamp and the username of the employee performing the action.

Marijuana and marijuana infused product waste must be made unusable and unrecognizable prior to leaving the Licensed Premises. Marijuana and marijuana infused product waste shall be rendered unusable and unrecognizable through grinding and incorporating the marijuana waste with non-consumable, solid wastes listed below such that the resulting mixture is at least 50 percent non-cannabis waste:

1. Paper waste;
2. Plastic waste;
3. Cardboard waste;
4. Food waste;
5. Grease or other compostable oil waste;

The facility shall utilize inventory tracking software to ensure its post-harvest waste materials are identified, weighed and tracked while on the Licensed Premises until disposed of.

All cannabis waste must be weighed before leaving any Licensed premises. The facility is required to maintain accurate and comprehensive records regarding waste material that accounts for, reconciles, and evidences all waste activity related to the disposal of cannabis. After the marijuana and marijuana infused product waste is made unusable and Unrecognizable, then the rendered waste shall be:

1. Disposed of at a solid waste site and disposal facility that has a Certificate of Designation from the local governing body;
2. Deposited at a compost facility that has a Certificate of Designation from the Department of Public Health and Environment; or
3. Composted on-site at a facility owned by the generator of the waste and operated in compliance with the Regulations Pertaining to Solid Waste Sites and Facilities in the Department of Public Health and Environment.

## Merit Criteria - Question 12

Product safety is paramount for business best practices, ensuring that all medical marijuana and manufactured medical marijuana products are safe for use or consumption by qualifying patients. KMD LLC will fully comply with Hawaii Administrative Rules, Chapter 11-850-75, concerning quality control, health, safety and sanitation standards as well as Sections 329D-8, 329D-10, and 329D-11, HRS. The six principles of product safety are quality assurance, environmental control, integrated pest management, cleaning and sanitation, consistent execution of all SOPs, and rigorous laboratory testing for potency; microbials, residual solvents, heavy metals, and toxins. As required within Chapter 11-850-71, Product and Product Standards, KMD LLC intends to establish and maintain a written policy and procedure that includes:

1. Safe and appropriate use of equipment;
2. Effective training and monitoring of employees and subcontractors who participate in the production of marijuana and manufactured marijuana products;
3. Adequate protocols for laboratory testing of marijuana;
4. Safe and appropriate storage and disposal or destruction of marijuana at all stages of production and sale, ensuring there is no diversion to unauthorized persons.
5. State compliant packaging and labeling

topping, de-fanning, pruning, and netting, human eyes provide the best initial source of identifying afflictions. Through daily scouting, cultivators will actively look for molds, mildews and other pathogenic outbreaks in order to be proactive with regard to the medical marijuana crop, instead of reactive. As the plants are harvested and transferred to trim, dry and cure, each department is actively looking for afflictions to the plants that may have escaped the notice of the cultivation team. Should an issue be discovered, the plant will be segregated and reported to the cultivation team who will, through BioTrackTHC, locate the flower room from which the plant came and look for any other issues in that room to treat and quarantine before it may spread throughout the production center.

Within the production center, KMD LLC will strive to maintain complete control over all environments containing marijuana or manufactured marijuana products. Controlling the environment is critical to the overall health of the facility. Deploying Stulz Air Technology HVAC Systems, or a similar cleanroom atmospheric control equipment, will aid in the creation of a nearly aseptic, exceptionally clean environment. These systems will provide all elements necessary to successfully creating and managing a controlled environment, including human management of temperature, humidity, and carbon dioxide levels.

Through adoption of a proper Integrated Pest Management (IPM) protocol, KMD LLC

Cleaning and sanitation of the facility and all equipment is another critical element with regard to product safety and maintaining a safe work environment both in the production center as well as retail dispensing facility (see Appendix 12 - Section 12.2 - Production Center Cleaning and Sanitation Practices). Wash stations, lockers and work clothing will be provided. Daily cleaning checklist will be used by staff to ensure compliance with regard to Chapter 11-850-75, quality control, health, safety, and sanitation standards.

Rigorous health, safety, and sanitation standard will also apply to staff or any other persons who may come in contact with medical marijuana and medical marijuana products while at the production center or retail dispensing facility. KMD LLC intends to ensure all licensed facilities are well-equipped to provide sanitary working conditions for staff, addressing all requirements set forth within Chapter 11-850-75. This includes but is not limited to; excluding contact from staff and persons with illness, open lesion or wounds, or any other source of contamination, providing ample hand washing facilities and hand cleaning preparations, and requiring all staff to conform to hygienic best practices while on duty. Additionally, no animals will be permitted within the facilities, except for service animals in accordance with section 34702.5, HRS. Additionally, KMD LLC will not alter marijuana or manufactured marijuana products to change their appearance, flavor, or smell in a way that would appeal to minors.



MSDS for every hazardous chemical on premise and make them available to employees as part of our Right-to-Know provisions – which says employees have the right to know about the chemicals to which they are exposed. The other key responsibilities we have are:

- Maintaining a hazard communication program detailing the plans in place for the safe handling of chemicals;
- Maintaining a written chemical inventory of every hazard chemical in the facility to which employees are exposed;
- Maintaining proper labels and warning signs associated with said chemicals;
- Training employees on chemical hazards and necessary precautions.

Retail dispensary staff will be required to use nitrile gloves whenever in contact with medical marijuana, to ensure there is no contamination between staff and the medical marijuana or manufactured marijuana products (see Attachment 2 - Section 12.3 - Retail Dispensing Location Cleaning and Sanitation Practices). KMD LLC will ensure dispensary agents maintain proper cleaning and equipment maintenance logs in a secured file to be readily available to the department of health or law enforcement for inspection as necessary. A cleaning checklist is an effective tool to ensure no essential cleaning and sanitation tasks are overlooked. KMD LLC will generate maintenance logs to be used within all licensed facilities and kept on file for inspection.

licensee shall ensure and verify that each sample is tested and analyzed for each of the items laid out in subsection (c) of Chapter 11-850-85, and may obtain results from different laboratories for different items if a laboratory cannot perform all the tests. Internal testing for chemical, microbiological, or other testing, as necessary to augment independent third party testing will help in the effort to provide safety to all involved parties. Using BioTrackTHC also ensures product safety, as after a testing laboratory has entered sample test results into the BioTrack system, the licensee retrieves the testing laboratory results and the System applies those results to the original lot from which the sample came. Only if the inventory item has a status of “Passed QA” can it be placed on a manifest. A registered organization user cannot, under any circumstances, place an item on the transportation manifest if that item requires testing and does not have a “Passed QA” status (e.g. not yet tested or failed testing). (see Merit Criteria - Question 9 and Appendix 9 - Section 9.1 - Microbial Testing Overview).

As an overarching precaution in the event a qualifying patient experiences any unwanted side-effect or adverse effects, “Business” will have a product alert and recall protocol in place (see Appendix 12 - Section 12.4 - Marijuana & Manufactured Marijuana Product Alert & Recall).

## **Merit Criteria - Appendix 12**

### **12.1 - Integrated Pest Management and Environmental Monitoring**

Regular environmental monitoring (EM) ensures the growing environment remains optimized, and helps detect potential problems early on to allow correction before they become serious or damaging. A history of EM data exposes causal factors related to environmental, disease, or pest problems. It can indicate if the environment control systems (such as the HVAC) have sufficient capacity to control the internal environment even when significant inter-seasonal fluctuations are happening in the outside environment. Regular data collection also reveals the effect of an environmental adjustment on the plants.

A critical element to EM is “scouting” for pests and pathogens. Scouting is by far the most critical element to Integrated Pest Management (IPM). Scouting is the process of actively inspecting each plant for afflictions or other alerts. During the vegetative stage of the plant lifecycle, including mother plants, daily watch for any alerts during cloning, watering, topping and transporting. Scouting by cultivation staff allows a production center to operate proactively versus reactively in regard to plant afflictions including pests and pathogens.

As with any other intensely cultivated and selectively bred agricultural crop, medical marijuana is beset by a number of pathologies that require immediate intervention to avoid

Integrated Pest Management (IPM). IPM programs combine cultural and environmental controls, regular EM and disease scouting, application of organic pesticides and fungicides, and application of treatment for established diseases and high pressure situations. The focus of an IPM program will largely depend on the options that are realistically available to the cultivator.

Resistance buildup can be avoided or delayed with proper treatment rotation, and residual levels in the product will be at (or preferably below) the EPA's residuals limits for hops and food crops. Hops is a reasonable parallel due to its close relation to the marijuana plant. All incoming plants must be quarantined for at least two weeks to ensure any diseases or pests they may have cannot spread into the production center. Quarantined areas must be under strict contamination control and monitored by trained staff.

### **Integrated Pest Management – Mother Plants and the Vegetative Phase**

Scouting is the most important part of IPM. During scouting, a cultivator is looking for any potential afflictions such as mold, powdery mildew, bug infestations or other pathogenic outbreaks. Scouting should be performed during cloning, watering, feeding, topping, transplanting and shuffling. The key is to identify a plant issue before it become an epidemic within the production facility. The culture that should be engendered is that of being proactive instead of reactive.

## **12.2 - Production Center Cleaning and Sanitation Practices**

Equipment that will typically come in contact with medical marijuana plants are pots, vegetative racks, transplanting tables, wheeled transport racks, flowering systems, trays, machine trimmer, scissors, drying racks and cure buckets. All these items need to be properly sterilized and disinfected prior to reuse. This is important as much to prevent the contamination of the equipment as it is for plants to not get contaminated through contact. Pots are reused once a plant has been harvested and removed from the pot. The old grow medium is removed from the pot and used to mix with discarded plant matter that is then sterilized as part of the destruction protocol. It must be rendered unusable and unrecognizable. The pot will be cleaned and sanitized to remove the salt-based nutrient sediments that form at the bottom of the pot through several months of nutrient feedings.

Vegetative racks house plants for eight to ten weeks and will have contamination built up through feeding runoff and pesticide, miticide, and fungicide management. Once the plants on the vegetative racks have moved on from this phase of their life-cycle to the flowering phase, these racks will have to be cleaned and sterilized. The transplanting tables that are used for repotting from a clone dome to a 1-gallon to a 5-gallon pot will likewise require cleaning and disinfecting.

trimmed product goes into large aluminum trays that will then be taken to the dry/cure department to dry for a week to 10 days. Once the trimmings have fully dried and have been stored or packaged, the aluminum trays can be reused once they have been thoroughly cleaned and disinfected. The machine trimmer will need to be cleaned each day after use. It is crucial that plants with powdery mold or mildew never go through the machine. Sticky resins will need to be removed and thoroughly sanitized prior to running plants through the next day.

The wire hanging racks will also be cleaned after the removal of fully dried flower and prior to repopulation. All cure buckets are used for the batching and curing of product. The product will cure in a bucket anywhere from two weeks to two months. After product is done curing and prior to repopulation, the buckets must be cleaned and disinfected. Sticky resins can form on the inside of the container and must be removed. A record of all cleaning should be maintained daily and weekly and should be held for six years.

KMD LLC will ensure cultivation staff maintain proper cleaning and equipment maintenance logs in a secured file to be readily available to the Department of Health for inspection as necessary. Everything in the facility needs to be cleaned with a State-approved sanitizing agent, including but not limited to: tables, racks, floors, walls, lighting hoods, fans, trays, buckets, pots, HVAC equipment, glass, and water system equipment to mitigate the risk of

janitorial service or in-house maintenance team will be called in weekly for thorough vacuuming and sanitation. Soap, water, rubbing alcohol and other sanitizing solutions will be used when cleaning. The person cleaning will also wear clean clothing, protective gloves and goggles and will be required to spray down with an alcohol spray solution prior to entering rooms in which medical marijuana is stored.

The equipment that will typically come in contact with medical marijuana and manufactured marijuana products within a retail dispensing facility are, but not limited to: display jars, chopsticks/tongs, scales, weighing trays, and holding containers. All of these items need to be properly sterilized and disinfected prior to reuse. This is important as much to prevent the contamination of the equipment as it is for the medical marijuana to not get contaminated through contact. Larger pieces of equipment and furniture, like display cases and furniture within the patient waiting area, will also be cleaned regularly by a professional cleaning service to ensure the utmost sanitation within the dispensary. Retail dispensary staff will be required to use nitrile gloves whenever in contact with medical marijuana and manufactured marijuana products to ensure there is no contamination.

#### **12.4 - Marijuana and Manufactured Marijuana Product Alert & Recall**

log format (logs to be maintained and shared by the Dispensary Manager and the General Manager) as well as the batch and other control information related to the suspect product.

**Stage 2:** Upon the second notice to a member of the retail dispensing facility by a qualified patient or authorized caregiver of a particular and specific negative effect (ex: persistent debilitating headaches) the Dispensary Manager shall note the reoccurrence of the same effect in log format, immediately notify the General Manager of the second similar occurrence, and ensure that the batch (or lot) present in the dispensary is quarantined in a separate secured location in a secured area. The General Manager (or in the absence of access to the General Manager, an approved member of the Management Team) shall immediately notify the supplied network of General Managers, Dispensary Managers, and/or Clinical Directors to quarantine the suspect batches (or lots) and shall cause a random sampling of two products within the suspect batch (or lot) to be submitted for immediate (expedited if available) third party laboratory testing for contamination of any kind.

If the testing results for both samples come back with no contamination indicators, the products under quarantine shall remain in quarantine for an additional five business days to insure there are no further reports of similar effects experienced by other qualified patients or authorized caregivers. Once the five business day period has passed with no similar reports, the



texts, and voicemail to ensure the return of the recalled product until all such products are returned or verified as having been consumed.

**Stage 3:** Upon serving notice to a member of the retail dispensing facility by a qualified patient or authorized caregiver of a third particular and specific negative effect (ex: persistent debilitating headaches) thought to be the result of ingestion of an approved marijuana or manufactured marijuana product, the Dispensary Manager shall note the effect in a common log format, immediately notify the General Manager of the third similar occurrence, and ensure that the batch (or lot) present in the dispensary is quarantined in a separate secured location. Upon this third incident, all products within the reference batches (or lots) shall be subject to an immediate recall notice to all qualified patients and authorized caregivers through use of the POS tracking system database to identify the aforementioned patients and authorized caregivers and will continue to follow up via email, texts, and voicemail to ensure the return of the recalled product until all such products are returned or verified as having been consumed.

*NOTE: Our seed to sale software provider, BioTrackTHC, has specifically designed elements within its software to assist as well as manage the overall recall process. KMD LLC will be relying upon these sales records for management of the process. (Please see the BioTrackTHC State referenced compliance elements for further delineation).*

### Merit Criteria – Question 13

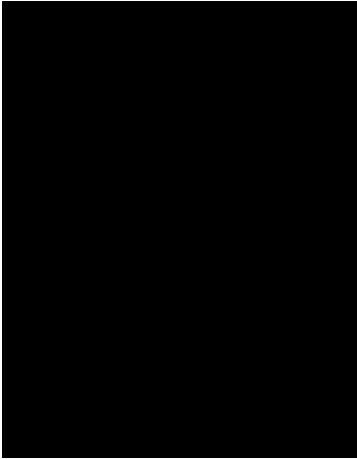
KMD LLC has no revocation of license history. Dr. Kellen Kashiwa has no history of having a license revoked. As a medical provider, Dr. Kashiwa is subject to numerous license requirements in order to treat patients and prescribe pharmaceuticals and has never had any license revoked professionally and personally.

As previously stated, KMD LLC is committed to providing equal access to safe, quality medical marijuana to qualified patients in a secure and professional environment in accordance with Chapter 329D, HRS and Hawaii Administrative Rules, Chapter 11-850. We will work collaboratively with the State of Hawaii, other dispensary licensees and the community we serve to ensure patient safety, product safety and public safety. KMD LLC is committed to delivering advanced, pharmaceutical grade medical marijuana through empathetic patient service, extensive clinical research, considerate clinical experience and education.

We realize that the regulations as it relates to medical marijuana are subject to change, therefore, we will benefit from the knowledge, education and experience of Anthony Suetsugu, attorney-at law as an advisor to our board. Mr. Suetsugu expertise in government relations and regulated entities as well as his background in Biology will prove invaluable as we navigate this new territory. (See Appendix 13)

## Appendix 13

### **Anthony Suetsugu, Attorney at Law**



Mr. Suetsugu is a Senior Associate at one of the top law firms in Hawaii – Kobayashi, Sugita, & Goda, where he focuses on commercial litigation, regulated entities, and corporate matters and was recently selected as a “Rising Star” by Super Lawyers, a rating service of outstanding lawyers from more than 70 practice areas who have attained a high-degree of peer recognition and professional achievement. A large part of his practice now involves advising companies in regulated industries, where he regularly interacts with many state and city agencies on behalf of public utilities, insurance companies, financial institutions, et al. He represents an array of clients, ranging from large national financial institutions seeking to provide services in Hawaii to small start-ups just breaking to island markets.

Mr. Suetsugu graduated from William S. Richardson School of Law, where he served as an editor of the law review, won multiple CALI Excellence for the Future awards (given to the highest scoring law students at many law schools), and completed a judicial externship with the Honorable Richard R. Clifton of the United States Court of Appeals for the Ninth Circuit.

Active in his community, Mr. Suetsugu serves on the Board of Directors of ClimbHI, a local nonprofit that works closely with organizations, such as, the Hawaii Tourism Authority to expose high school students from low-income communities to various career options throughout the state. He also coaches football and soccer at various levels throughout Honolulu.

Prior to attending law school, Mr. Suetsugu attended Claremont McKenna College in Claremont, CA, where he received a Bachelor of Arts degree in Biology and Government and co-authored and published “Determination of Reference Ranges for Transcutaneous Oxygen and Carbon Dioxide Tension and the Oxygen Challenge Test in Healthy and Morbidly Obese Subjects” in the Spring 2008 edition of the Journal of Surgical Research.