SACVALLEY MEDSHARE	POLICY: *System Security Practices*	POLICY NUMBER: *SVMS-18.001*
Compliance Requirement	Author: Elizabeth L. Steffen	Origination Date: 10/06/2015
HIPAA 45CFR 164.308 . 310 .312 Ca Civil Code 56	Revised By:	Revised Date:

Policy Statement:

SacValley MedShare(SVMS) shall protect the security and privacy of all information entrusted to it. The primary goal of the four sections outlined in this policy are:

- *To effectively manage the risk of security exposure or compromise within the systems.*
- *To communicate the responsibilities for the protection of information.*
- *To establish a secure processing base and a stable processing environment.*
- *To promote understanding and compliance with all applicable laws and regulations.*
- *To protect SVMS Board and Staff and preserve their options in the event of an information asset misuse, loss, or unauthorized disclosure.*

Section I: Information Governance & Risk Analysis
Section II: Information Security
Section III: Sanctions & Education
Section IV: Contingency Plan

Authorization	Name	Signature	Date
Board Chair	Myron MacNeil		11/5/15
Compliance Officer			
Executive Director			

Reference:
Central Illinois Health Information Exchange Security Policies. (2011, December).

Attachment(s):

A: *Security Agreement (1 page) (page 10)*
B: *Verbal Warning (1 page) (page 11)*
C: *Written Warning (1 page) (page 12)*
D: *Employment Suspension (1 page) (page 13)*
E: *Termination of ePHI Access; Letter to Staff (1 page) (page 14)*
F: *User Change of Access Form (1 page) (page 15)*
G: *Termination of Employment; Letter to Staff (4 pages) (page 16)*
H: *User Termination of Access Form (1 page) (page 20)*
I: *Annual User Review (1 page) (page 21)*
J: *Information Asset Inventory (1 page) (page 22)*
K: *Employment Verification (1 page) (page 23)*
L: *New User Access Form (1 page) (page 24)*
M: *Visitor Log Template (1 page) (page25)*

Version	Date	Author	Comment
.001	11/05/2015	E. Steffen/Dr. Dorsey-Tyler/J. Helvey	Initial release.

Section I: Information Governance & Risk Analysis

Privacy and Security management shall be performed by the Executive Director and designated staff as needed. In the absence of an Executive Director, the Board of Directors shall designate an individual to cover such duties. They shall be responsible for establishing and maintaining privacy and security policies and making recommendations to the Board of Directors.

Responsibilities:

- Make recommendations to the Board with regard to privacy, confidentiality and security policies and practices.
- Review and recommend modification of privacy, confidentiality and security policies and practices in light of operating experience, changes in law, and changes in available compliance tools.
- Participate in incident response to contain, investigate, and prevent future privacy, confidentiality or security breaches.
- Maintain working relationships with legal counsel and outside consultants and use the services of such parties to assist with responsibilities.
- Maintain working relationships with the privacy and security officers and managers of SVMS Participants.
- Lead privacy, confidentiality and security awareness and training initiatives to educate workforce and users about risks.
- Direct and review the findings from risk assessments and audits of information systems and privacy and confidentiality practices.

It is the responsibility of the Executive Director to take the roles of Security and Privacy for SVMS.

Risk Analysis

SVMS shall conduct an initial risk assessment to identify foreseeable threats and vulnerabilities that present potential risks to the confidentiality, integrity, and availability of the Electronic Protected Health Information (ePHI) entrusted to its care. Based on that assessment, SVMS shall adopt and implement reasonable safeguards to protect such ePHI, including protection of the CIHIE information systems where EPHI is received, aggregated, stored, or transmitted. SVMS shall also conduct subsequent risk assessments, as appropriate, and add to or modify its safeguards to meet any identified gaps or new risks.

When evaluating, selecting, rejecting and implementing safeguards, the following factors should be considered:

- Safeguards for the protection of the privacy and security of confidential information and ePHI should be targeted to foreseeable threats to the privacy or security of such information.
- Safeguards should be reasonable. They should be designed to prevent improper access to, or use and disclosure of, confidential information or ePHI by workforce and others, but they should not interfere with SVMS's ability to conduct its business.
- Safeguards should be reasonably affordable. It is appropriate to engage in cost benefit analysis. SVMS recognizes that it will not always be able to select the most effective

solution in an area due to the cost of the solution or the potential detriment to other areas of compliance or operations that may result.

- Safeguards must be evaluated within the resources and capabilities of the organization. These are SVMS's responses to perceived threats to the privacy and security of information at SVMS, and they should be tailored to fit SVMS's specific needs.
- The selection of safeguards, such as the assessment of risk, is to be regarded as dynamic in light of SVMS's operating and compliance experience and understanding of applicable laws and regulations. All compliance steps should be open to reevaluation and change. Criticism and suggestions should be encouraged.
- Certain implementation specifications set forth in the HIPAA Security Rule are classified as "Addressable." CIHIE shall meet these implementation specifications. In the event that it is not reasonable and appropriate to meet an addressable implementation specification, then the Executive Director shall document why it would not be reasonable and appropriate to implement the specification and recommend an equivalent alternative.

All software purchases, upgrades and development relative to ePHI shall take into account potential impact on applicable information security laws, statutes and regulations, including HIPAA compliance.

The Executive Director shall ensure that a risk assessment be conducted. The risk assessment shall:

- Comply with security audit guidelines set forth by NIST, ISO 27001, or similar protocols.
- Be approved by the Board of Directors.
- Identify the potential threats and vulnerabilities that pose a risk to the confidentiality, integrity, and availability of critical data and information technology.
- Identify potential security measures (i.e. safeguards) to mitigate such risks and vulnerabilities.
- Identify areas where SVMS's current security measures (i.e. safeguards) fail to satisfy the requirements of the HIPAA Security Rule and other applicable information security laws, statutes and regulations.
- The risk assessment will be conducted periodically and whenever significant changes occur in the SVMS information technology environment.

Section II: Information Security

Acceptable Use

All use of SVMS information technology is to be in compliance with all policies and procedures and sound business judgment. SVMS shall monitor e-mail, Internet use, and other computer resources.

Logon access will be administered to only those staff members and authorized users that

- follow the applicable log-on authorization procedure, and
- are actually authenticated as authorized users.

Use of the Internet, e-mail and other uses of computer resources must always be able to withstand public scrutiny and not cause legal liability or embarrassment to SVMS.

Staff members shall be made aware that they should have no expectation of privacy when using SVMS resources or networks to access anything.

Electronic Mail

- SVMS shall employ virus protection software on all machines to prevent transmission of viruses.
- E-mail that is not secure or encrypted should not be used to send electronic protected health information or confidential information.

Unacceptable uses of CIHIE's information technology include, but are not limited to:

- Violation of the privacy of other users and their data.
- Violation of the legal protection provided by copyright and licensing laws applied to programs and data.
- Attempts by members to monitor or intercept the files or electronic communications of other members or third parties.
- Attempts by members to hack or obtain access to systems or accounts they are not authorized to use.
- Use of others' log-ins or passwords.
- Use of electronic media in a manner that is likely to cause network congestion or significantly hamper the ability of other members to access and use the system.
- Use inconsistent with laws, regulations or accepted community standards. Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.
- Intentionally or knowingly releasing a virus or other program that damages, harms, or disrupts a system or network.
- Violation of the integrity of computing systems.
- Use of the SVMS facility for fund-raising or public relations activities unrelated to an individual's employment by SVMS.
- Malicious or disruptive use, including use of the SVMS facilities or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses or other malicious software, and use to make unauthorized entry to any other machine accessible via the network.
- Using SVMS resources for unauthorized or illegal purposes or knowingly accepting or using information which has been obtained by illegal means.
- Use in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use.
- Misrepresentation of one's self or SVMS.
- Accessing or attempting to access data or information without proper authorization even if it is not securely protected.
- Obtaining, possessing, using or attempting to use someone else's password regardless of how the password was obtained.
- Sending an overwhelming number of files across the network (e.g., spamming, e-mail blasting or denial of service attacks).
- Preventing others from accessing services.

- Users are not permitted to install any unapproved software or attach any device to workstation/laptop without specific approval.

Users are responsible for installing and using virus protection routines and installing patches and updates.

Users must ensure that computer repairs are undertaken in a manner that protects the confidentiality of data stored in the system.

Users should never open e-mail from an unknown, suspicious or untrustworthy source nor download any attachments from such e-mail.

Users should delete Spam, chain, and other junk e-mail without opening or forwarding such e-mail.

SVMS Information Resources are to be used primarily for business purposes and only for the performance of one's job responsibilities.

Occasional and reasonable non-business usage of systems may be allowed at the discretion of the Executive Director and/or Board Chair provided that such usage:

- Does not interfere with work performance or productivity of oneself or others.
- Does not consume more than a trivial amount of resources that could otherwise be used for business purposes.
- Does not endanger the privacy or security of protected health information or confidential information.
- Is not contrary to SVMS Policies, standards or procedures.

Users are responsible for exercising good judgment regarding the reasonableness of personal use.

If there is any uncertainty on whether a use is appropriate or allowed, the User should consult the Executive Director.

Activity Review

SVMS shall review information systems activity on a periodic basis to determine whether ePHI is accessed or disclosed inappropriately. Examples of information system activity records may include, but are not limited to, audit logs, access reports and Security Incident reports. The Executive Director and Board Chair shall specify audit requirements, the frequency of such audits and the individual and/or firm responsible. Any Security Incidents identified as a result of information systems activity review shall be investigated. The Executive Director shall:

- Conduct random security audits, and
- Perform complaint-based investigation.

The findings from these review activities shall be reported to the Board of Directors.

Passwords

Strong passwords shall be used, changed as directed, and protected. All staff should be aware of how to select strong passwords.

1. All system-level passwords (e.g. administrative level accounts, etc.) must be changed on at least a quarterly basis.
2. All user-level passwords must be changed at least every ninety (90) days.
3. All passwords must conform to the guidelines described below.
    (a) Strong passwords must be used wherever technically feasible.
    (b) Password Requirements include:
        i. Must be 10 characters in length

ii. Must contain at least one number, upper-case letter, and symbol.
iii. Must not be a dictionary word
iv. Must not contain the user's name or login ID.

(c) DO NOT:
i. Reveal a password to ANYONE in any form, including other SVMS staff or Directors.
ii. Use the same password for SVMS accounts as for any non-SVMS accounts.
iii. Talk about a password in front of others

4. If an account or password is suspected to have been compromised, report the incident to the Executive Director.
5. Access to the health information exchange data:
   (a) Each user of the HIE shall have a unique identification. Where users are accessing the HIE remotely (i.e. "offsite" from the Participant's "HIE authorized" network,) the system shall provide a method to accurately identify the user through a two-factor authentication process.
   (b) A self-service password recovery process may be used.
   (c) A Participant may perform password management for its users.
   (d) A Participant may employ a single sign-on process for its users.

Personnel Security

SVMS shall ensure that all personnel (internal staff and independent contractors) requiring access to ePHI have appropriate access rights.

- All personnel requiring access to ePHI shall be identified.
- Appropriate job description will be signed. *Job descriptions will be maintained by the Executive Director and/or Board Chair/designee.*
- Authorization to access ePHI shall be granted as necessary based on job functions (SVMS-FORM-053, Attachment L).
- Access to ePHI shall be granted based upon roles performed and shall be supervised by the Executive Director or Board Chair.
- Access levels shall be reviewed periodically and when there are personnel status changes.
- All personnel having access to ePHI shall undergo an appropriate background investigation prior to employment. Such check may include, but shall not be limited to, a credit check, verification of references and a criminal background check (SVMS-FORM-052, Attachment K).
- All personnel having access to ePHI shall be subject to ongoing, periodic background checks.
- Documentation regarding background checks, personnel actions, and the levels of access granted to each member should be maintained for no less than seven (7) years.
- Temporary personnel are treated as staff. Contractors may be subject to these personnel security elements.
- Upon termination, the following tasks will need to be completed:
  - Recover from the SVMS personnel all keys and access tokens for facilities, buildings, offices, desks and file cabinets etc.

- Disable all personnel network access, e-mail accounts, and access to all other systems.
- If the SVMS personnel had system level or administrative access to systems, and/or remote access; change system passwords for all systems containing or allowing access to sensitive information.
- Change the SVMS personnel's voice mail message to include directions regarding who or whom to contact.
- Review all electronic files and forward or destroy, as appropriate.
- As appropriate, notify customers and vendors with ongoing issues or projects involving the former SVMS personnel member that such member is no longer employed.

Physical Access

Physical safeguards will be implemented to protect SVMS personnel, information, equipment, and other assets. Reasonable and appropriate controls will be installed to control and validate each individual's access to facilities based upon their role or function. Individuals may not enter areas where protected health information or confidential information is stored unless authorized.

Visitors will be required to sign in and wear badges within SVMS facilities. A visitor log (SVMS-FORM-054, Attachment M) should be maintained and include:

- The visitor's name.
- The name of the employer or affiliation.
- The name of the official authorizing entry (the person visited).
- The specific zone entered.
- The date and time of entry.
- The date and time of departure.

Terminals, workstations, and/or laptops should be located in a secure area and also be positioned in such a way as to eliminate unauthorized overview. Appropriate logs and records of access will be maintained.

Privacy and Security Incident

All Privacy or Security Incidents shall be reported to the Executive Director who shall take appropriate steps to block further incidents, repair and restore service, and preserve evidence.

Any information concerning a known or suspected privacy or security breach (an "Incident") must be reported to the Executive Director without delay and in writing. The Security manager will inform the appropriate Participant Privacy and Security Contacts. In addition, the Executive Director may, after consultation with legal counsel, report the incident to outside law enforcement authorities whenever this is required to comply with legal requirements, rules or regulations.

The Executive Director is responsible for managing mitigation efforts. Specifically, to:

- Block or prevent continuation of the Incident, if possible.
- Repair the resulting damage and fix and/or delegate the fix of the root cause.
- Restore service to its former level, if possible.
- Preserve evidence, where appropriate.

Upon receipt of written notice, the Executive Director shall, without delay, identify and record any damage caused, and restoration or repair required, as well as gather all of the necessary information required to prosecute the Incident, if applicable. They will develop a detailed plan to effectively remedy and respond to all reported Incidents pursuant to this policy. The Executive Director will follow the Breaches of Protected Health Information Procedure (SVMS-PRO-003).

If a Participant's information, workforce member or user was involved in an Incident, then the Executive Director will report such Incident to the Privacy and Security contacts designated by that Participant.

The Executive Director will coordinate with the Participant's Privacy and Security contacts in responding to the Incident.

The appropriate response to an Incident will be determined by the Executive Director and the appropriate Participant's Privacy and Security contacts and will based on the potential and/or actual impact of the Incident.

Any harmful effects of the Incident will be mitigated to the extent practical.

All Incidents shall be reported to the Board of Directors on a periodic basis.

Workstation/Laptop Administration

All workstations owned or operated by SVMS shall be used in a manner to safeguard the confidentiality and integrity of protected health information and confidential information. All information assets shall be logged on the Information Asset Inventory Form (SVMS-FORM-051, Attachment J).

Users shall sign off of their equipment at the end of each work day. Workstations/Laptops will automatically lock after fifteen (15) minutes of inactivity. Users are responsible for performing required software updates on their respective machines.

Section III: Sanctions and Education

Sanctions

SVMS shall apply sanctions to staff who violate HIPAA Security Compliance policies/procedures and/or SVMS policies/procedures. Staff shall agree to comply with all policies/procedures and this sanctions policy by signing the Security Agreement, SVMS-FORM-042 (Attachment A).

Types of Sanctions:

- Verbal warning (SVMS-FORM-043, Attachment B)
- Written warning (SVMS-FORM-044, Attachment C)
- Employment suspension (SVMS-FORM-045, Attachment D)
- Termination of access to Electronic Protected Health Information
  - Termination Letter to staff (SVMS-FORM-046, Attachment E)
  - Change of User Access Form for system changes (SVMS-FORM-047, Attachment F)
- Termination of Employment.
  - Termination Letter to staff (SVMS-FORM-048, Attachment G)
  - Change of User Access Form for system changes (SVMS-FORM-049, Attachment H)

Education

- All staff must be informed of all policies and procedures and their responsibilities in writing. All new staff will sign a statement acknowledging they have received and read the policy and understand their responsibilities.
- All users shall be informed that any actions taken under their assigned identification, such as a user "ID," are their responsibility.
- A signed statement indicating awareness, compliance, and intent of continued compliance with all policies and procedures will be required upon annual review (SVMS-FORM-050, Attachment I) of each staff member with access to critical systems or sensitive information.
- Important aspects of any information security and privacy policies and procedures will be communicated on a regular basis through postings, distributions, logon screens, meetings or other means that provide regular and useful reminders concerning information security and privacy policies and standards.
- Persons responsible for information technology resources must be aware of the information security and privacy policies and procedures and must be knowledgeable about effective security practices for the technical environment under their control. In particular, such individuals shall be trained regarding password maintenance, incident reporting and viruses and other forms of malicious software.

Section IV: Contingency Plan

All HIE data is stored at ICA and is backed up and covered under their disaster recovery plan. SVMS physical paper documentation, agreements, contracts, etc. shall be scanned onto Box.com. The Executive Director and Technical Lead laptops will have remote wipe capabilities and no data will be stored on local hard drives.

Attachment A: Security Agreement

SACVALLEY MEDSHARE

Security Agreement

The success of SacValley MedShare (SVMS) and the privacy of all patients and Participants depend upon the protection of their information against theft, destruction, or disclosure to outside interests. As an employee, contractor, business associate, consultant, or vendor for SVMS, you may be required to operate computer equipment and/or have access to software systems. Therefore, you must understand and adhere to the information security policies described below, which are in effect. This document meets the Health Insurance Portability and Accountability Act standards in regard to privacy and security.

- Operating or attempting to operate computer equipment without specific authorization, appropriate training, and appropriate security access is prohibited. Training for designated computer applications is required prior to system access.
- Demonstrating the operation of computer equipment to anyone without written authorization is prohibited.
- Using the computer system, equipment, and functions for uses other than the performance of job duties is prohibited.
- Disclosing any portion of SVMS's computerized information system to an unauthorized individual is prohibited. This includes, but is not limited to, computer design, programming techniques, flow charts, source code, screens, and documentation created by SVMS employees or outside sources.
- Maintaining the confidentiality of passwords that allow access to the computer system is required.
- Disclosing a password to anyone, at any time, for any reason, is prohibited and considered a violation of this agreement. If accidental password disdosure occurs, the Executive Director should be contacted immediately. The password will be deleted, and following an investigation, a new password will be issued.
- Recording of passwords in any manner is prohibited and considered a violation of this agreement.
- Disclosing or accessing any portion of a patient's record, except in the specific circumstances mentioned below or when authorized by the patient, is prohibited. Access to any portion of a patient's record and information is limited to health care professionals directly involved in the patient's care, those monitoring the quality of the patient's care, non-clinical employees maintaining patient records or the operating system, or agents of SVMS performing services for SVMS under agreement.

Each employee is responsible to report activity that is contrary to the provisions of this agreement to the Executive Director and/or Board Chair. Failure of to comply with the above policies will result in formal disciplinary action, up to and including termination. Failure of consultants and/or vendors to comply with the above policies may result in the termination and/or cancellation of this agreement and shall not affect the severability of any other agreements between the parties.

Electronic Mail (eMail), Intranet, and Internet Use: "The use of the Internet and Intranet is reserved for those activities that use this medium as a method to access financial, clinical, and information that furthers assigned duties of the individual. While the Internet connectivity and the bandwidth provided by SVMS can be used for simple inquiries to obtain pertinent financial news and current events, the amount of usage is monitored closely and at any time can be restricted for such casual usage to reserve aforementioned bandwidth for critical application uses. Any use of this service that would be deemed unlawful, obscene, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability or otherwise violate any federal, state or local law is also prohibited. Such determination is the sole discretion of SVMS.

Signature: _____ Date: _____

Printed Name: _____

SVMS-FORM-042.001 Security Agreement

Page 1 of 1

Attachment B: Verbal Warning

SACVALLEY MEDSHARE

Verbal Warning

Employee: _____
Last Name First Name

Job Title: _____

Date of Warning: _____

This notice of verbal warning is issued for the following reason(s):

_____

_____

_____

_____

_____

_____

_____

_____

Previous Notice of Warning: _____ Type: ☐ Verbal ☐ Written

Employee Comments:

_____

_____

_____

_____

Reviewer

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

Employee Receipt of Notice

Employee Signature: _____ Date: _____

Printed Name: _____

SVMS-FORM-043.001 Verbal Warning

Page 1 of 1

Attachment C: Written Warning

SACVALLEY MEDSHARE

Written Warning

Employee: _____
Last Name First Name

Job Title: _____

Date of Warning: _____

This notice of written warning is issued for the following reason(s):

_____

_____

_____

_____

_____

_____

_____

_____

Previous Notice of Warning: _____ Type: ☐ Verbal ☐ Written

Employee Comments:

_____

_____

_____

_____

Reviewer

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

Employee Receipt of Notice

Employee Signature: _____ Date: _____

Printed Name: _____

SVMS-FORM-044.001 Written Warning Page 1 of 1

Attachment D: Employment Suspension

SACVALLEY MEDSHARE

Employment Suspension Notice

Employee: _____
Last Name First Name

Job Title: _____

This notice is to notify you that you have been suspended from your employment, without pay, for a period of _____ day(s), for the following dates:

_____ through _____, to return to work on _____.

This notice of suspension is issued for the following reason(s):

_____

_____

_____

_____

_____

_____

_____

Employee Comments:

_____

_____

_____

_____

Reviewer

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

Employee Receipt of Notice

Employee Signature: _____ Date: _____

Printed Name: _____

SVMS-FORM-045.001 Employee Suspension Notice

Page 1 of 1

Attachment E: Termination of ePHI Access; Letter to Staff

SACVALLEY MEDSHARE

Termination of ePHI Access

Employee: _____
Last Name First Name

Job Title: _____

This notice is to notify you that your access to ePHI has been terminated for the following reasons:

_____

_____

_____

_____

_____

_____

_____

After full investigation, access may or may not be granted.

Reviewer

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

Employee Receipt of Notice

Employee Signature: _____ Date: _____

Printed Name: _____

SVMS-FORM-046.001 Termination of ePHI Access

Page 1 of 1

Attachment F: User Change of Access Form

SACVALLEY MEDSHARE

User Change of Access Form

Effective Date: _____

Name: _____ Title: _____

Vendor: ☐N ☐Y: _____ (Vendor Name)

Changes Requested

New Title: _____ New Supervisor: _____

Hardware Needed: ☐ Y ☐ N Type of HW: _____

Type of Change:

☐ Software Needed _____
List Software & note reason

☐ Network Share(s) _____
List

☐ CareAlign Portal ☐ Email Addr. ☐ Administrative ☐ Box.com

☐ Other _____
Explain

☐ Model After User: _____

Authorization

Submitted By: _____ Date: _____
Signature & Title

Approved By: _____ Date: _____
Signature & Title

IT Use Only

Reviewed By: _____ Processed By: _____
Initials *Date* *Initials* *Date*

SVMS-FORM-047.001 User Change of Access Form Page 1 of 2

Attachment G: Termination of Employment; Letter to Staff – Page 1

SACVALLEY MEDSHARE

DATE

NAME
ADDRESS

Dear *NAME*:

This is to advise you that your employment will terminate effective, *DATE*, due to *(those reasons discussed with you)* **OR** *(a change in business conditions/performance concerns/ organizational fit/etc.)*.

We would also like to take this opportunity to remind you that, notwithstanding the termination of your employment with SVMS, certain obligations under your signed security agreement and other agreements that you may have signed during your employment with SVMS continue. These obligations include, but may not be limited to, obligations of confidentiality and obligations relating to any intellectual property to which you may have contributed while employed by SVMS.

If you have any questions concerning the information contained in this letter, please contact me directly.

Yours sincerely,

Name
Title

I, _____, hereby accept the terms set out in Appendix "A", in full and final satisfaction of any claims that I may have.

_____ _____
Signature Date

SVMS-FORM-048.001 Termination of Employment Page 1 of 4

Attachment G: Termination of Employment; Letter to Staff – Page 2

SACVALLEY MEDSHARE

APPENDIX A

Termination Agreement between *SacValley MedShare* and *(EMPLOYEE NAME)*

This Agreement confirms the circumstances surrounding the termination of your employment with *SacValley MedShare*, known as "*SVMS*".

1. Termination Date
Your employment with SVMS will terminate effective **DATE**.

2. Vacation
Any outstanding vacation owing will be paid to you as a lump sum, less applicable taxes, etc. Payment will be paid upon execution of this agreement.

3. Expenses
SVMS will reimburse you for all reasonable business expenses incurred, up to and including **(TERMINATION DATE)**, provided you submit appropriate forms and supporting original receipts no later than ten (10) days from the date of this executed agreement.

4. Change of Address
In the event that you change your address, please notify SVMS via email at support@sacvalleyms.com so that we can arrange to forward your tax and wage information to the correct address.

5. References
At your request, we will provide you with a letter confirming your employment with SVMS, according to our usual practices.

6. Return of Company Property
Upon termination of your employment, you are required to return all SVMS property and material in your possession and are not to retain copies of such materials.

7. Release
All payments are conditional upon your having signed, witnessed, dated and returned the attached copy of this letter and the Release form (Appendix "B") to SVMS by ***DATE***.

SVMS-FORM-048.001 Termination of Employment

Page 2 of 4

Attachment G: Termination of Employment; Letter to Staff – Page 3

SACVALLEY MEDSHARE

APPENDIX B

RELEASE

WHEREAS the undersigned (the "**Releasor**") was an employee of SacValley MedShare (the "**Company**");

AND WHEREAS the Releasor's employment with the Company has been terminated,

NOW THEREFORE THIS AGREEMENT WITNESSETH that the receipt and sufficiency of payments due is hereby acknowledged, the Releasor covenants and agrees as follows:

1. FULL AND FINAL RELEASE

The Releasor does hereby release and forever discharge the Company, its successors, administrators, assigns, affiliates and related companies, and their directors, officers and employees (the "**Released Parties**") of and from all actions, causes of action, damages, claims, cross claims and demands whatsoever, (including all damage, loss and injury not now known or anticipated but which may arise in the future and all effects and consequences thereof), however and wherever arising, which the Releasor had, now has, or which the Releasor, its heirs, administrators and assigns or any of them hereafter can, shall or may have in respect of the Releasor's employment by the Company or the termination thereof.

The Releasor further agrees not to make or continue any claim or take or continue any proceeding against the Released Parties in Canada or elsewhere in the world, with respect to the employment of the Releasor by the Company or with respect to the termination of the Releasor's employment.

The Releasor warrants that the Releasor has disclosed to the Company any and all human rights complaints, concerns or issues arising out of or in respect of the Releasor's employment at the Company.

It is understood and agreed that both this release and any consideration transferred hereunder are deemed to be no admission whatsoever of liability on the part of the Released Parties.

2. CONFIDENTIALITY UNDERTAKING

The Releasor, intending to be legally bound, hereby further agrees and undertakes to protect in strict confidence, and not to use or disclose, any and all information relating to the terms and the fact of this Release.

It is further understood that the Releasor will continue to be bound by any and all confidentiality agreements signed by the Releasor while in the employ of the Company, and the Releasor recognizes that the full force of penalties and consequences pertaining to the breach of said agreements remain in full force.

3. BENEFIT OF RELEASE, AGREEMENT AND UNDERTAKING

It is understood and agreed that this Release shall ensure to the benefit of the Released Parties and shall be binding on the Releasor, the Releasor's successors, administrators, assigns, affiliates and related companies.

The Releasor acknowledges that the signing of this Release is not a condition for the Releasor to receive any money to which the Releasor would otherwise be entitled to by operation of statute.

SVMS-FORM-048.001 Termination of Employment Page 3 of 4

Attachment G: Termination of Employment; Letter to Staff – Page 4

SACVALLEY MEDSHARE

The Releasor hereby declares that it fully understands the terms of this settlement, has had the opportunity to obtain independent legal representation in connection with this Release and that it voluntarily accepts same for the purpose of making full and final compromise, adjustment and settlement of all claims as aforesaid, whether arising by force of contract, at common law, or under applicable statutes.

IN WITNESS WHEREOF this agreement has been executed before the undersigned witness by the Releasor on the ____ day of _____, 20*XX*.

SIGNED, SEALED AND DELIVERED)
SIGNED in the presence of)

_____)
WITNESS)
Name: _____)

_____
RELEASOR
Name: _____

SVMS-FORM-048.001 Termination of Employment

Page 4 of 4

Attachment H: User Termination of Access Form

SACVALLEY MEDSHARE

User Termination of Access Form

Effective Date: _____

Name: _____ Title: _____

Vendor: ☐N ☐Y: _____ (Vendor Name)

eMail Address: ☐ Remove ☐ Forward To: _____

Voice Mail: ☐ Remove ☐ Forward To: _____

Personal Data ☐ Remove ☐ Reassign To: _____

Windows Account: ☐ Delete ☐ Disable: Reason: _____

CareAlign Portal ☐ Disable _____

List ID(s)

Administrative ☐ Remove ☐ Disable: Reason: _____

Box.com Access ☐ Remove ☐ Disable: Reason: _____

Equipment Returned ☐Y ☐N ☐N/A _____

If Yes; list equipment type and serial number

Notes: _____

Authorization

Submitted By: _____ Date: _____

Signature & Title

Approved By: _____ Date: _____

Signature & Title

IT Use Only

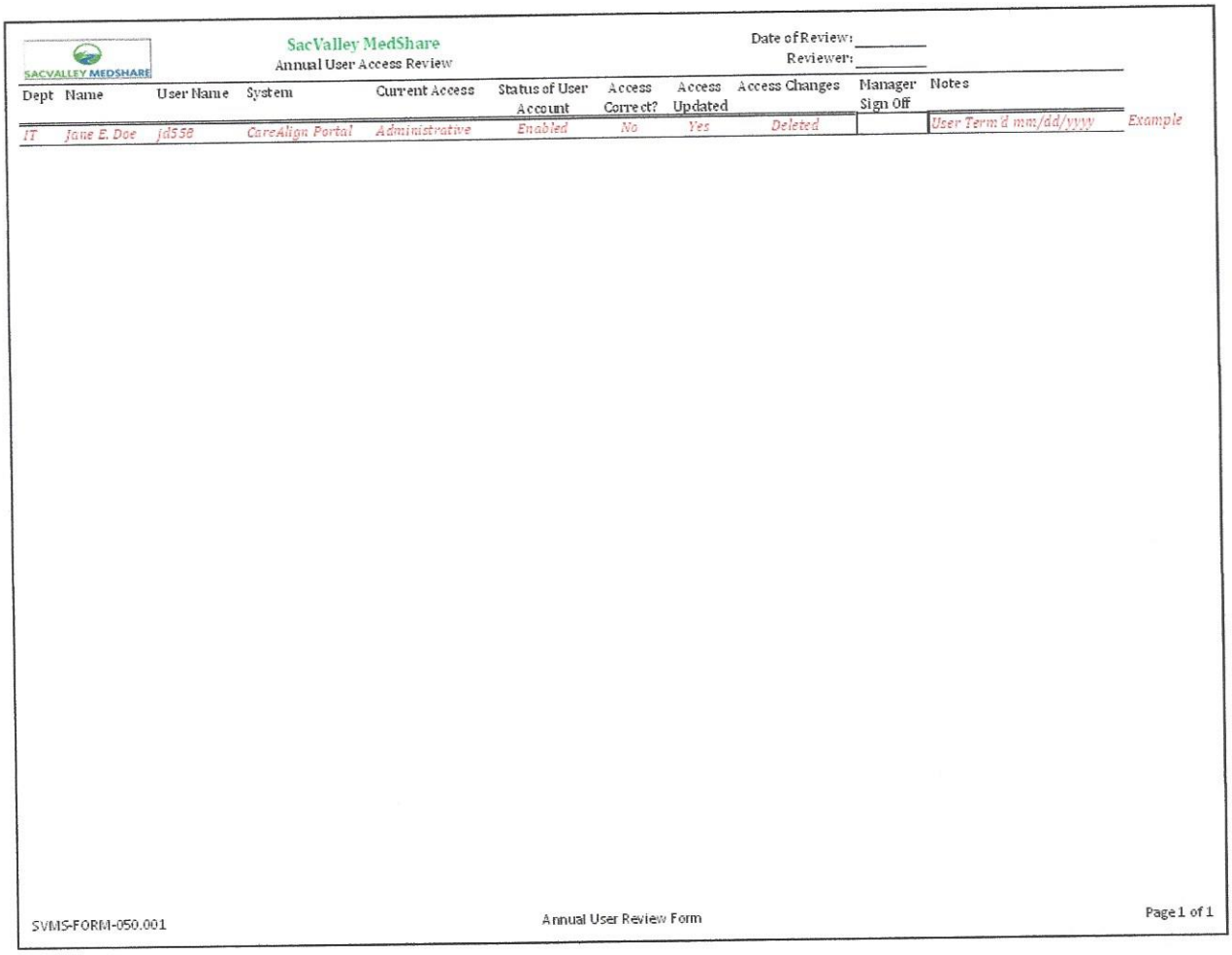
eMail Address:	*Windows Account*	*CareAlign Portal*
☐ Address Removed	☐Removed ☐ Disabled	☐ Disabled
☐ Forwarded To:	*Box.com Access*	☐ Disabled ☐ Removed
Equipment Returned: ☐Y ☐N ☐N/A	*Personal Data*	
Equipment Wiped: ☐Y ☐N	Stored: _____	

Reviewed By: _____ *Initials* *Date*

Processed By: _____ *Initials* *Date*

SVMS-FORM-049.001 User Termination of Access Form Page 1 of 1

Attachment I: Annual User Review Form



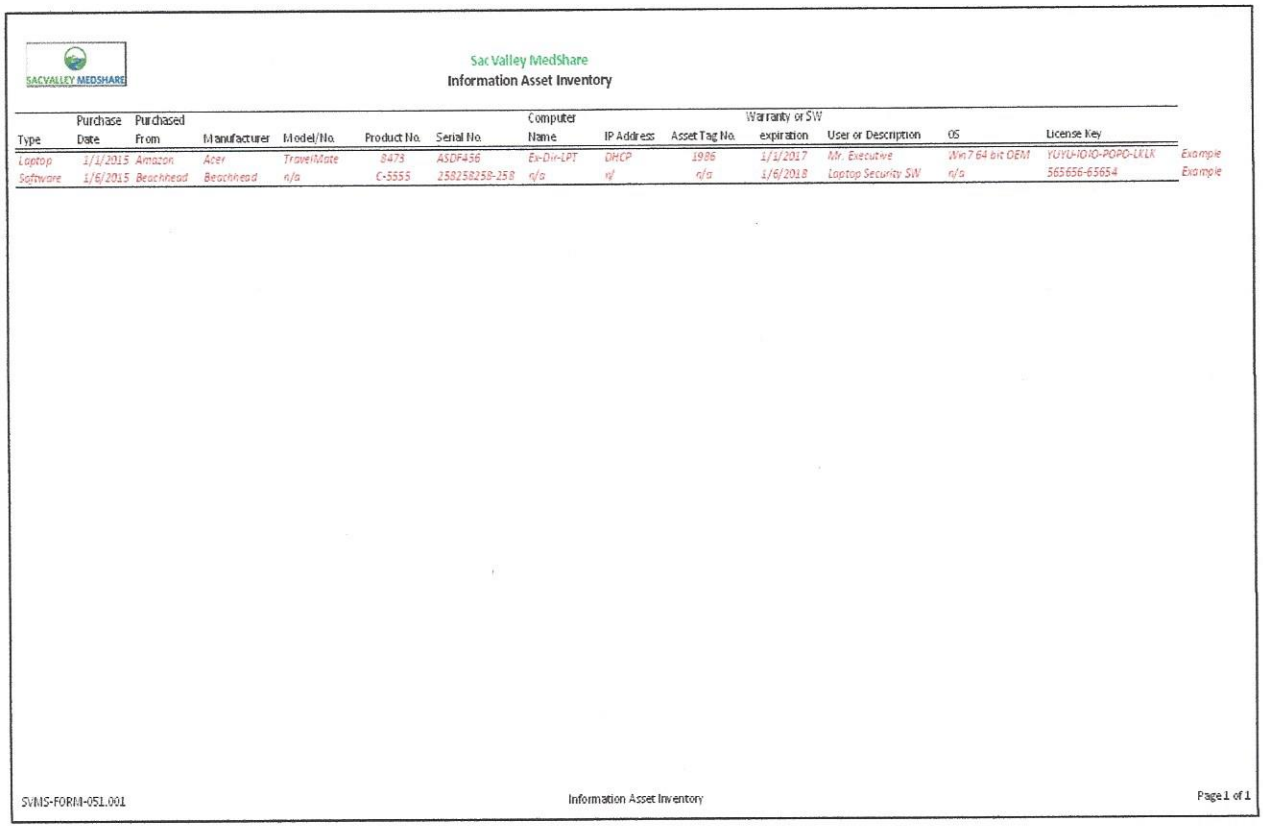
SacValley MedShare
Annual User Access Review

Date of Review: _____
Reviewer: _____

Dept	Name	User Name	System	Current Access	Status of User Account	Access Correct?	Access Updated	Access Changes	Manager Sign Off	Notes	
IT	*Jane E. Doe*	*jd558*	*CareAlign Portal*	*Administrative*	*Enabled*	*No*	*Yes*	*Deleted*		*User Term'd mm/dd/yyyy*	*Example*

SVMS-FORM-050.001 Annual User Review Form Page 1 of 1

Attachment J: Information Asset Inventory



SACVALLEY MEDSHARE

Sac Valley MedShare
Information Asset Inventory

Type	Purchase Date	Purchased From	Manufacturer	Model/No.	Product No.	Serial No.	Computer Name	IP Address	Asset Tag No.	Warranty or SW expiration	User or Description	OS	License Key	
Laptop	*1/1/2015*	*Amazon*	*Acer*	*TravelMate*	*8473*	*ASDF456*	*Ex-Dir-LPT*	*DHCP*	*1986*	*1/1/2017*	*Mr. Executive*	*Win7 64 bit OEM*	*YUYUHOIO-POPO-LKLK*	*Example*
Software	*1/6/2015*	*Beachhead*	*Beachhead*	*n/a*	*C-5555*	*258258258-258*	*n/a*	*n/*	*n/a*	*1/6/2018*	*Laptop Security SW*	*n/a*	*565656-65654*	*Example*

SVMS-FORM-051.001 Information Asset Inventory Page 1 of 1

Attachment K: Employment Verification

SACVALLEY MEDSHARE

Employment Verification

Applicant: _____
Last Name First Name

Job Title: _____

☐	Resume Received	
☐	Interview Conducted and Documentd	
☐	Completed Employment Eligibility Verification Form; I-9	
☐	Completed Federal/State Withholding Form; W-4	
☐	Signed Job Description	
☐	Signed Security Agreement	*SVMS-FORM-042*
☐	Signed SVMS Policy & Procedure Acknowledgement	*SVMS-FORM-014*
☐	*Criminal Background Check completed*	Initials:_____
☐	*Reference Check completed*	Initials:_____
☐	*Credit Check completed*	Initials:_____

By signing below, you are stating that all of the above forms have been returned back and signed by the employee if applicable.

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

Applicant Approved/Disapproved for hire. (circle one)

If Disapproved, state reason(s): _____

_____

_____

SVMS Signature: _____ Date: _____

Printed Name: _____ Title: _____

SVMS-FORM-052.001 Employment Verification

Page 1 of 1

Attachment L: New User Access Form

SACVALLEY MEDSHARE

New User Access Form

Start Date: _____

Name: _____ Title: _____

Vendor: ☐N ☐Y: _____ (Vendor Name)

Equipment Needed? ☐ Y ☐ N _____

If Yes; specify equipment and if in budget purchase

eMail Address: ☐Y ☐N Voice Mail: ☐Y ☐N Box.com: ☐ Y ☐ N

Software Needed: ☐ Base ☐ HR ☐ CareAlign Portal ☐ Administrative ☐ Other: _____

Base Programs are: Microsoft Office Suite, WinZip, Adobe Reader

Network Shares: _____

List Shares to give access to

Model After: _____

Notes: _____

Authorization

Submitted By: _____ Date: _____

Signature & Title

Approved By: _____ Date: _____

Signature & Title

IT Use Only

eMail Address: _____ @sacvalleyms.org _____ *pwd*	*Windows Account* ID: _____	*CareAlign Portal*	
Network Shares: _____ _____	*Administrative* ID: _____		*Box.com* *ID:*
Notes: _____			
Reviewed By: _____ *Initials* *Date*		Processed By: _____ *Initials* *Date*	

SVMS-FORM-053.001 New User Access Form Page 1 of 1

Attachment M: Visitor Log Template

SACVALLEY MEDSHARE

Visitor's Log

Date	Time In	Name of Visitor	Company	Person Visiting	Time Out	Signature of Visitor

SVMS-FORM-054.001 Visitor's Log Template

Page 1 of 1