SACVALLEY MEDSHARE	POLICY: *Auditing of Access to and Use of HIE Information*	POLICY NUMBER: *SVMS-14.001*
Compliance Requirement	Author: Elizabeth L Steffen	Origination Date: 11/04/2015
45 CFR § 164.308(a)(1)(ii)(D), 308(a)(5)(ii)(c), 312(b), 530(c)(1); 68 Fed. Reg. at 8355 & 8347	Revised By:	Revised Date:

Purpose and Principles:

The purpose of the Auditing of Access to and Use of HIE Information policy is to ensure that logging and audit practices for a Health Information Exchange (HIE) are in place and practiced.

Policy Statement:

SVMS shall:

- Ensure that all auditable activites within the HIE are logged, reviewed, and stored according to all applicable state and federal regulations,
- Periodically review audit logs and retain such audits for a period of no less than seven (7) years, and/or,
- Provide Participants with audit logs upon their request within a reasonable timeframe.

The attached *Audit and Accountability Checklist* (a one-page Microsoft® Excel® worksheet, printed to PDF, signed, and scanned back as PDF) is complete for the SVMS vendor, Informatics Corporation of America (ICA) and ICA's system meets all criteria as specified by local, state, and federal regulations.

Authorization	Name	Signature	Date
Board Chair	Myron Machula	Myron Machula	12.3.15
Compliance Officer			
Executive Director			

Attachments:

Attachment A: *Signed SVMS/ICA Audit and Accountability Checklist (1 page) (Page 2)*

Reference:

Markel Foundation. (2015, November). *P7 Logging and Audit Controls* Retrieved November 3, 2015 from http://www.markle.org/health/markle-common-framework/connecting-professionals/p7

NC HIE. (2015.) *NC HIE Privacy Policy* Retrieved November 3, 2015 from http://www.nchie.org/providers/privacysecurityframework/

Version	Date	Author	Comment
.001	12/03/2015	E. Steffen	Initial release.

Attachment A: Signed SVMS/ICA Audit and Accountability Checklist

SACVALLEY MEDSHARE

SacValley MedShare

Audit and Accountability Checklist

11-4-15 date init.

Compliance Requirement: 45 CFR §164.308(a)(5)(ii)(C)

Informatics Corporation of America (ICA) Hybrid Data System	Yes	No	N/A
1. The system is required to log users' system login and logoff with date and time, or, if the system does not have the capability to record login/logoff activity, it may rely on an external security system's access control logging function to record access.	✓		
2. The system must have the ability to log read, create, update, delete, forward, and print access initiated by individuals and processes for systems containing confidential and restricted data. For data warehouses, data marts, and operational data stores, the system must have the ability to log queries, or alternatively the tables read must be logged. Row-level logging must be available on demand.	✓		
3. All audit records must be identified by a unique record key or number, and include: User identifier/name of user Time/date Device identifier (when used to access) Source (i.e. subsystem or system of origin of the event [access request]) Type of action (e.g. read, write, update, delete, or copy) or access for diagnostic purposes.	✓		
4. Unsuccessful login attempts and access violations within the system must be logged.	✓		
5. Security administrative functions must be logged.	✓		
6. System administrative functions must be logged.	✓		
7. Audit records must be protected against unauthorized access, modifications, and deletion.	✓		
8. Audit records must be readily available for 90 days and archived for a minimum of two years, or up to the six years used for the archiving of HIPAA disclosures.	✓		
9. Security administrators and auditors can request or generate reports which may consist of any or all of the audit record elements for any or all types of actions.	✓		

Originally completed in Summer 2013, documented in November 2015.

SVMS-FORM-056.001 Audit and Accountability Checklist Page 1 of 1