SACVALLEY MEDSHARE 42 USC §13402, 45 CFR 164.404, 508, 528(a)(2); CA Civil Code §1785.11.2, 1798.29, 82, 84; CA Health & Safety Code §1280.15; CMIA (Civil Code 56.06)	PROCEDURE: *Breaches of Protected Health Information/Incident Response Procedure*	PROCEDURE NUMBER: *SVMS-PRO-003.001*
	Author: Elizabeth L Steffen	Origination Date: 01/08/2015
	Revised By:	Revised Date:

Purpose:

To ensure that all participant's notifications of breaches of Protected Health Information are investigated timely and according to applicable state and federal laws and regulations and to ensure that SacValley MedShare (SVMS) completes proper incident response through governance, triage, scoping, execution, and remediation of reported incidents.

Scope:

SVMS shall:

- Cooperate in investigations conducted by the Participant,
- Notify other participants or authorized users as needed to prevent further harm, or to enlist cooperation in any investigation, and/or mitigation of the breach,
- Cooperate in any mitigation steps initiated by the participant,
- Furnish audit logs and other information needed for the investigation,
- Assist with development and dissemination of remediation plans to strengthen safeguards or hold Participant's accountable, And,
- Any other identified, mutually-agreed upon steps as appropriate under specific circumstances.

Procedure:

1. Receipt of Notification from notifying entity:
    a. Receiver of notification shall:
        i. Log the incident on the Incident Response Log, (Attachment A, Microsoft® Excel ® worksheet, SVMS-FORM-007.)
            1. Assign Incident Number of next cronological number
            2. Input:
                - Date of Report (when the incident is being logged),
                - Notification Means (how was the notification received),
                - Incident Handler (who is leading the investigation),
                - Incident category level:
                    i. I = low risk
                    ii. II = medium risk
                    iii. III = high risk
                - Date of Incident (when incident occurred),
                - Time of Incident (time incident occurred), And,
                - Incident Description (brief summary of what is being investigated).
        ii. Forward notification and incident number to the SVMS Privacy Officer by the next business day after receipt of notice.
2. Investigation Steps
    a. Receive notification from *SVMS Privacy Officer.*
    b. *SVMS Privacy Officer* shall provide full cooperation with notifying entity.
    c. *SVMS Privacy Officer* shall complete the HIPAA Breach Risk Assessment form (Attachment B, Microsoft® Word ® document, SVMS-FORM-008.)to determine:

i. A system, application, or PHI was breached,
ii. Was unsecured PHI invovled,
    1. Yes, If PHI involved was encrypted, there is no breach to report and the process stops here and jumps to step 2-e.
    2. Yes, If PHI involved was identified, continue.
iii. SVMS Privacy Officer shall complete the Breach/Incident Report Form (Attachment C, Microsoft® Word® document, SVMS-FORM-0009) and continue to use it throughout the investigation.

d. Notification

Timeliness of Notification: California Department of Health and Human Services (CDHHS) shall be made within **fourteen (14)** calendar days of discovery and is the responsibility of the Participant if they are the notifying entity.

If SVMS is the discoverer, it is the responsibility of SVMS to make the proper report to CDHHS within the applicable timeframe.

1. Ensure within 3 business days whether or not a breach did or did not occur.
2. If a breach occurred, a phone call to necessary SVMS board and/or committee members must be made and documented in the log.
3. If a breach did not occur, ensure that incident is completed within ten (10) business days.
4. Continue to Step 2-e.

Notices:

Individual: The individual, or next of kin, whose PHI was breached shall be notified in writing by first-class mail using Breach Notification to Individual Form, (Attachment D: Microsoft® Publisher® document, SVMS-FORM-011).and include:

1. A description of the breach,
2. A description of the types of information that were involved in the breach,
3. The steps affected individuals should take to protect themselves from potential harm,
4. A brief description of what SVMS is doing to investigate the breach and mitigate harm, And,
5. Contact information for SVMS incident handler.

Media: For breaches involving more than five hundred (500) individuals, immediately an *in no case later than fourteen (14) calendar days following the discovery of a breach*, contact prominent media in an outlet serving each applicable state or juridiction whose unsecured PHI SVMS reasonably believes to have been accessed, acquired, or disclosed during the breach. The Executive Director is responsible for developing appropriate press released to be submitted to prominent media. The content shall include the same information as for the Indivdual notice. (Attachment D: Microsoft® Publisher® document, SVMS-FORM-010).

Notice to the Secretary: Notice of a breach shall be provided to the Secretary of Health and Human Services (HHS) by visiting the HHS website at: https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage and filling out the proper form, printing it to PDF for SVMS files, and submitting the form electronically to the Secretary. If the breach involved more than five hundred (500) individuals, immediately an *in no case later than sixty (60) calendar days following the discovery of a breach.* If the breach involved less than five hundered (500) individuals, the incident response log must be submitted annually to the Secretary, electronically through the website.

e. SVMS Privacy Officer Shall complete the Breach/Incident Report Form (Attachment C, Microsoft® Word® document, SVMS-FORM-0009) and continue to use it throughout the investigation.
f. Collect evidence and document information collected in the log:
    i. Incident Report Form,
    ii. HIPAA Breach Risk Assessment Form,
    iii. Breach/Incident Report Form,
    iv. Information Technology forensic evidence (reports, logs, audits),
    v. Communication records (phone logs, electronic mail, letters),
    vi. Law enforcement agency and/or police reports if applicable, And/Or
    vii. Legal counsel guideance if applicable.
g. Note determination in the log.
h. Document all efforts in the log.
i. Deliver any logs, reports, notes, and/or documents to notifying entity and archive all documents for SVMS.
j. Assist notifying entity with any and all remediation efforts as needed.

Authorization	Name	Signature	Date
Board Chair	Myron Machula	Myron Machula	12·3·15
Executive Director			

Reference:

American Health Information Management Association. (2009). *Template: Health Information Privacy and Security Breach Notification Letter.* Retrieved January 13, 2015, from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045987.pdf

California Hospital Association Appendix PR 12-B. (2013, June). *HIPAA Breach Decision Tool and Risk Assessment Documentation Form.* Retrieved January 13, 2015, from http://www.calhospital.org/sites/main/files/file-attachments/appendix_pr_12-b_2.pdf

Seneca Healthcare District HIPAA Breach Investigation and Notification of Unsecured PHI and Response Policy. (2013, December).

Seneca Healthcare District Incident Response Form. (2014, April).

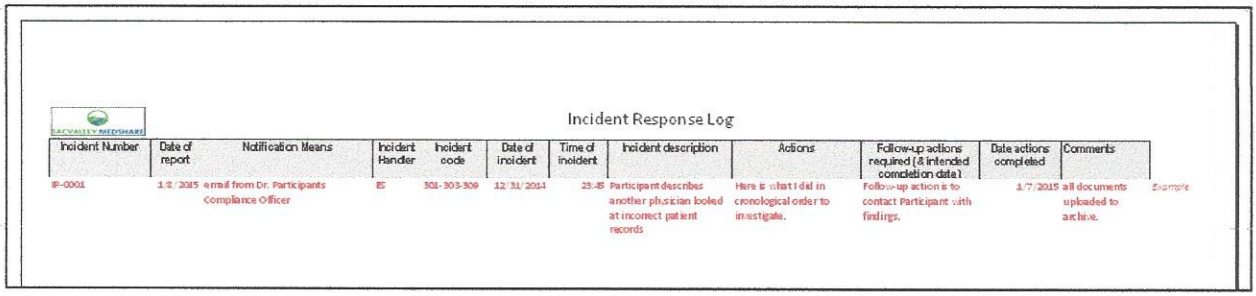
SACVALLEY MEDSHARE 42 USC §13402, 45 CFR 164.404, 508, 528(a)(2); CA Civil Code §1785.11.2, 1798.29, 82, 84; CA Health & Safety Code §1280.15; CMIA (Civil Code 56.06)	PROCEDURE: *Breaches of Protected Health Information/Incident Response Procedure*	PROCEDURE NUMBER: *SVMS-PRO-003.001*
	Author: Elizabeth L Steffen	Origination Date: 01/08/2015
	Revised By:	Revised Date:

Attachment(s):

A: *Incident Response Log (1 page) (page 5)*
B: *HIPAA Breach Risk Assessment (4 pages) (page 6-9)*
C: *Breach/Incident Report Form (1 page) (page 10)*
D: *Breach Notification to Media (1 page) (page 11)*
E: *Breach Notification to Individual (3 pages) (page 12-14)*

Version	**Date**	**Author**	**Comment**
.001	12/03/2015	E. Steffen/C. Kitzman/D. LeFevre/K. Dorsey-Tyler	Initial release.

Attachment A: Incident Response Log



Incident Response Log

Incident Number	Date of report	Notification Means	Incident Handler	Incident code	Date of incident	Time of incident	Incident description	Actions	Follow-up actions required (& intended completion date)	Date actions completed	Comments
IR-0001	1/8/2015	email from Dr. Participants Compliance Officer	ES	301-303-309	12/31/2014	23:45	Participant describes another physician looked at incorrect patient records	Here is what I did in cronological order to investigate.	Follow-up action is to contact Participant with findings.	1/7/2015	all documents uploaded to archive.

Example

Attachment B: HIPAA Breach Risk Assessment (page 1)

SACVALLEY MEDSHARE

HIPAA BREACH RISK ASSESSMENT FORM

Incident #: _____

Name of person completing form: _____

Date incident occurred: _____ Date incident detected: _____

Brief summary of incident, including number of patients affected: _____

_____

1. **Was protected health information (PHI) involved?** *(PHI is health information (including demographic information) that identifies, or there is a reasonable basis to believe it can be used to identify, the individual. Health information includes any information relating to the physical or mental health or condition of an individual, the health care provided to an individual, or payment for health care provided to an individual. PHI does not include employment records held by a hospital in its role as employer or PHI regarding a person who has been deceased for more than 50 years.)*

   ☐ Yes, PHI was involved. *Continue to Question 2.*

   ☐ No, PHI was not involved. No breach reporting required under HIPAA.

   Describe the information involved: _____

   _____

2. **Was the PHI unsecured?** *("Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance, such as ecryption or destruction. The guidance can be found on the DHHS website at www.hhs.gov/ocr/privacy/hipaa/ administrative/breachnotificationrule/brguidance.html.)*

   ☐ Yes, the PHI was unsecured. *Continue to Question 3.*

   ☐ No, the PHI was secured. No breach reporting required under HIPAA.

   Describe the PHI (for example, was it verbal, paper or electronic? Encrypted in compliance with NIST, password protected, other?): _____

   _____

3. **Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule?** *(Providers should keep in mind that a violation of the "minimum necessary" standard is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. Providers may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule.)*

1

Attachment B: HIPAA Breach Risk Assessment (page 2)

☐ Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. *Continue to Question 4.*

☐ No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

Describe who acquired, accessed, used and/or disclosed the PHI, whether the person(s) was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed: _____

_____

_____

4. **Does an exception apply?** Check any box below that applies:

☐ **Exception A.** A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

(i) Was made in good faith; and

(ii) Was within the course and scope of authority; and

(iii) Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce" includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether or not they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

☐ **Exception B.** A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

☐ **Exception C.** A breach does not include disclosure of PHI where the provider or business associate has a good faith belief than the unauthorized person who received it would not reasonably have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.)

☐ Yes, an exception applies. No breach reporting required under HIPAA.

☐ No, an exception does not apply. *Continue to Question 5.*

5. **Risk assessment.** An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL of the factors listed below.)

Factor A. Consider the nature and extent of the PHI involved, including the types of identifiers (and

2

Attachment B: HIPAA Breach Risk Assessment (page 3)

the likelihood of re-identification if the PHI is de-identified). *(Consider whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, STD, cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interests. Hospitals should also determine whether there is a likelihood that the PHI could be re-identified (if the PHI is de-identified) based on the context and the ability to link the information with other available information.)*

Describe the PHI involved, including identifiers and likelihood of re-identification (if the PHI is de-identified): _____

_____

_____

Consider whether PHI could be used in a manner adverse to the patient(s) or to further the unauthorized person's interests: _____

_____

_____

Factor B. Consider the unauthorized person who used or received the PHI. *(This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information - for example, is the person a covered entity required to comply with HIPAA, or a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.)*

Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified): _

_____

_____

Factor C. Consider whether the PHI was actually acquired or viewed. *(If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.)*

Describe whether the PHI was actually acquired or viewed (attach report from a computer forensic analyst, if one was obtained): _____

_____

Factor D. Consider the extent to which the risk to the PHI has been mitigated — for example, as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) has been completely returned, or has been/will be destroyed. *(Hospitals should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results in terms*

3

Attachment B: HIPAA Breach Risk Assessment (page 4)

of the risk to PHI. For example, a hospital may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)

Describe risk mitigation steps taken: _____

_____

_____

Factor E. Describe any other relevant factors (write "none" if appropriate): _____

_____

_____

Based on the factors noted above, is there a low probability that the PHI has been compromised?

- ☐ Yes (there is a low probability), thus **No** breach reporting required under HIPAA.
- ☐ No (there is not a low probability; there is a higher probability) thus breach reporting is required under HIPAA.

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether reporting is required under federal law (HIPAA). State laws require notification of a breach as defined in state law regardless of the results of this risk assessment. *(See "IV. State Law: Breach of Unencrypted Computerized Data in Any California Business" on page 12.2, and "V. State Law: Breach in a Licensed Health Care Facility" on page 12.4, for information regarding notification under state law.)* A provider may also have reporting obligations pursuant to a business associate agreement or other contract.

Signature of person completing this form: _____

Title: _____ Date: _____

4

Attachment C: Breach/Incident Report Form

SACVALLEY MEDSHARE

Incident Report

Incident Report #: _____

Section I: Patient/Subject Information

Patient/Subject Name: _____ Date and Time of Occurrence: _____

Notified by: _____ Today's Date: _____

Section II: Incident Details

Account of Incident: _____

Print name and title of person reporting _____ Date _____

Witness _____

Name Address Telephone Relationship

Section III: Action Taken

Actions _____

Conclusions _____

Recommendations _____

Print name and title of person doing follow-up _____ Date _____

OCCURRENCE INFORMATION

SECURITY (1)
300 ☐ Loss of Property
List: _____
301 ☐ Breach in Security
302 ☐ Theft of Information
999 ☐ Other _____

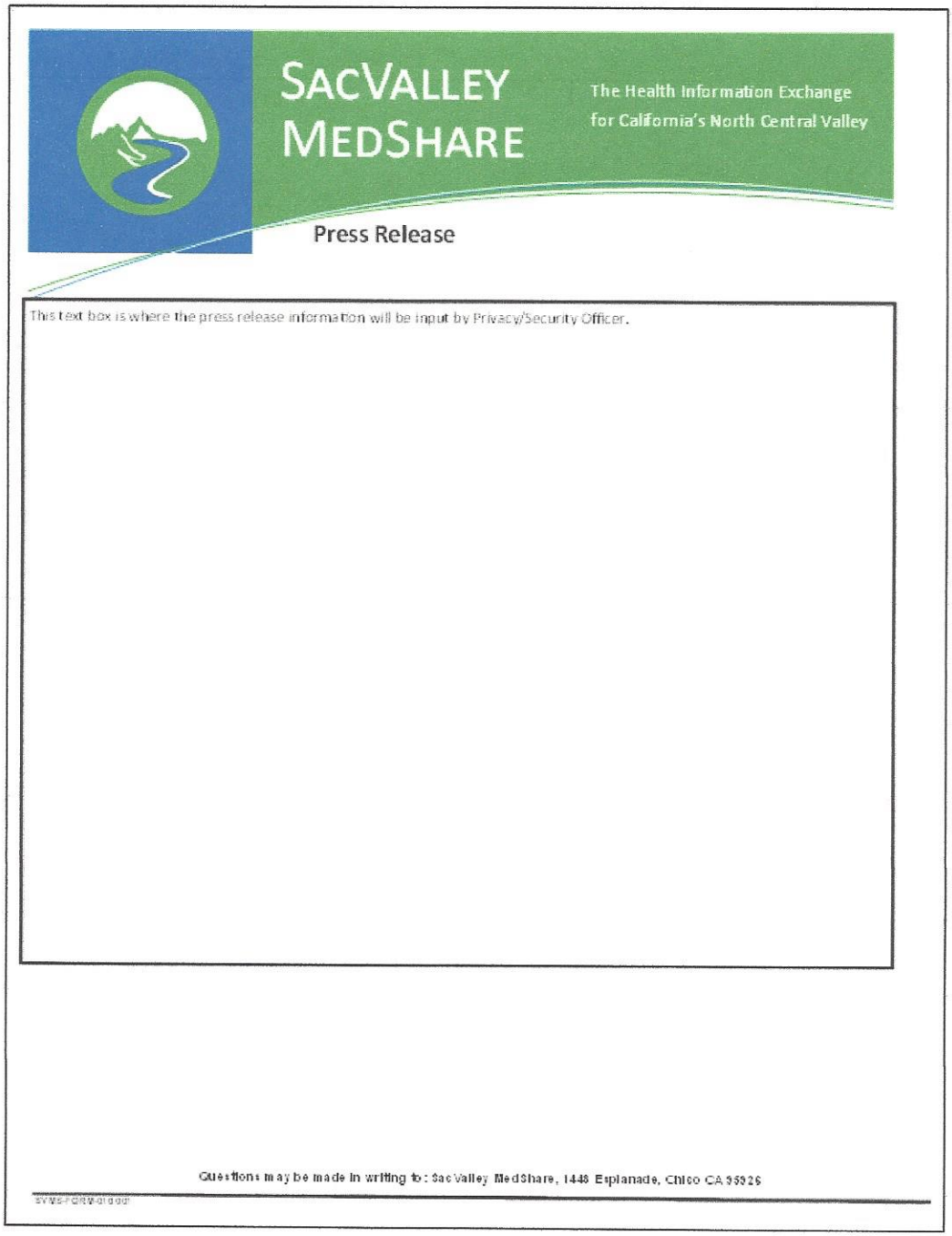
COMPLAINT (1)
303 ☐ Patient
304 ☐ Family/Visitor
305 ☐ Physician
306 ☐ Employee
307 ☐ Participant
308 ☐ Business Associate
999 ☐ Other _____

RELATED TO (1)
309 ☐ Confidentiality
310 ☐ Privacy
999 ☐ Other _____

SVMS-FORM-009.001 Breach/Incident Report Form

Page 1 of 1

Attachment D: Breach Notification to Media



Attachment E: Breach Notification to Individual (page 1)

SACVALLEY MEDSHARE

1448 Esplanade
Chico, CA 95926
info@sacvalleyms.org

[Date]

[Victim or Representative Name]
[Address Line 1]
[Address Line 2]
[City, ST Zip Code + 4]

Re: Personal [Health] Information of [Name of Victim]

Dear Sir/Madam,

On [date], [name of responsible healthcare organization] became aware of a breach of [your/loved one's] personal health information. We [have identified/estimate] the date of information leakage to be [date]. OR [The duration of information exposure was (include date range and time range)]. OR [We are unable to determine the date of the breach occurrence.] We are notifying affected individuals in as timely a manner as possible so you can take swift personal action along with our organization's efforts to reduce or eliminate potential harm. [It was necessary to delay notification because of the protected nature of the forensic investigation.] Incident investigation [is/is not] complete at this time.

The incident involving protected health information was [loss/theft/other] [state the circumstances]. [Examples: theft of a laptop containing files of 5,326 individuals from the trunk of a car OR exposure of personal health information on the (name of organization) Web site OR misplacement of five boxes, 250 paper medical records, during transit to a vendor destruction site]. The unsecured information includes [list the types of information involved: part/complete medical records dated between (state date range),
full name, Social Security Number, date of birth, home address, account number, diagnosis, types of treatment information, disability code, name other information types].

Attachment E: Breach Notification to Individual (page 2)

SACVALLEY MEDSHARE

The Health Information Exchange for California's North Central Valley

We recommend immediate steps be taken to protect [yourself/your loved one] from [additional/potential] information breach harm [List fitting recommendations such as:

- Register a fraud alert with the three credit bureaus listed here; and order credit reports:
  Experian: (888) 397-3742; www.experian.com; PO Box 9532, Allen, TX 75013
  TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790
  Equifax: (800)525-6285; www.equifax.com; PO 740241, Atlanta, GA 30374-0241
- Monitor account statements, EOBs, and credit bureau reports closely
- Contact the California Department of Consumer Affairs: Consumer Information Division 1625 North Market Blvd, Ste N 112, Sacramento, CA, 95834
- (If the consumer has validation their information has been compromised) Notify law enforcement to assist the investigation: [Provide advice on how to file and provide contact information for local law enforcement, the state attorney general office, and the Federal Trade Commission]
- Access helpful Web links to learn additional information on consumer protection when personal information is compromised. [List Web links or provide own organization's Web site] [For example, include AHIMA's Medical Identity Theft Response Checklist for Consumers: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039114.pdf]

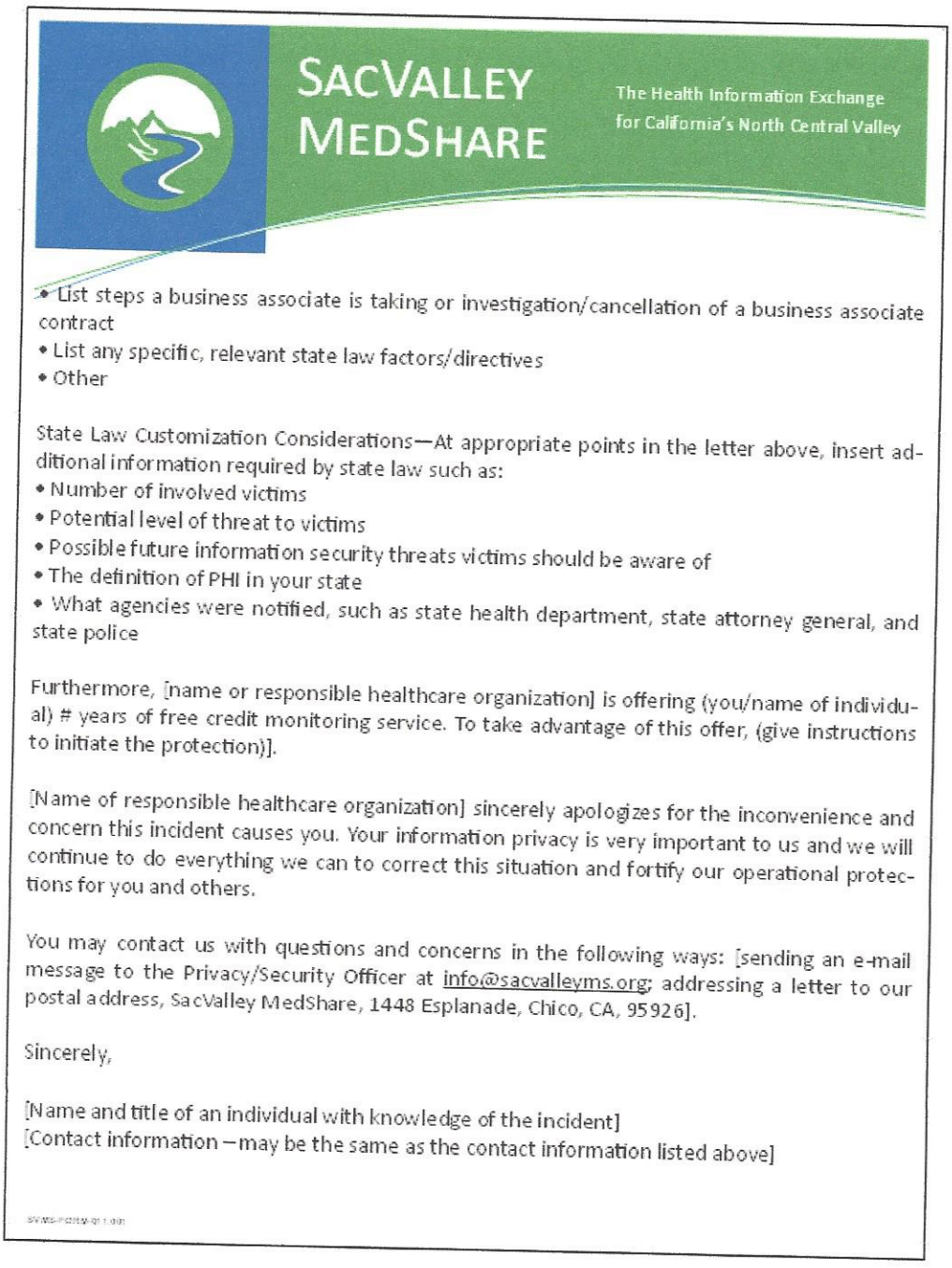
[Name of responsible healthcare organization/s] [has/have taken OR will soon take] these steps to protect your, and others', personal information from further harm or similar circumstances: [Choose from or customize these examples or add your own]:

- Initiated a forensics security investigation
- Filed a police report on [date]; Initiated a criminal investigation
- Address operational or technology updates or changes triggered by the incident to improve and/procedures

- Sanctioned five employees/a physician by suspension/termination of employment/medical staff privileges

SVMS-FORM-001.001

Attachment E: Breach Notification to Individual (page 2)



SACVALLEY MEDSHARE

The Health Information Exchange for California's North Central Valley

- List steps a business associate is taking or investigation/cancellation of a business associate contract
- List any specific, relevant state law factors/directives
- Other

State Law Customization Considerations—At appropriate points in the letter above, insert additional information required by state law such as:

- Number of involved victims
- Potential level of threat to victims
- Possible future information security threats victims should be aware of
- The definition of PHI in your state
- What agencies were notified, such as state health department, state attorney general, and state police

Furthermore, [name or responsible healthcare organization] is offering (you/name of individual) # years of free credit monitoring service. To take advantage of this offer, (give instructions to initiate the protection)].

[Name of responsible healthcare organization] sincerely apologizes for the inconvenience and concern this incident causes you. Your information privacy is very important to us and we will continue to do everything we can to correct this situation and fortify our operational protections for you and others.

You may contact us with questions and concerns in the following ways: [sending an e-mail message to the Privacy/Security Officer at info@sacvalleyms.org; addressing a letter to our postal address, SacValley MedShare, 1448 Esplanade, Chico, CA, 95926].

Sincerely,

[Name and title of an individual with knowledge of the incident]
[Contact information—may be the same as the contact information listed above]