	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 4.1.2</b>
	<b>Title: INCIDENT RESPONSE PROCEDURE FOR PERSONAL DATA ABOUT CALIFORNIA RESIDENTS</b>	<b>Page: 1 of 9</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/31/03</b>

**Incident Response Procedure for Personal Data about California Residents**

**I. SCOPE**

This procedure applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This procedure applies to all Tenet information assets and information asset Users.

**II. PURPOSE**

To establish procedures for identifying and reporting unauthorized access to personal data and for notifying those individuals whose information may have been compromised. California legislation Senate Bill 1386, effective July 1, 2003, requires all organizations that collect certain personal information regarding residents of California to protect it against possible “identity theft”. In addition, if an incident occurs that involves the compromise of unencrypted personal information, individuals whose personal information may have been compromised must be notified.


Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception will be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

**III. PROCEDURE**

A. General

This document provides guidance regarding how to respond to instances of unauthorized access to personal information as well as improper distribution of personal information. For the purpose of this procedure, personal information is defined to mean the first name OR first initial and last name of a resident of California in combination with one or more of the following:

- a) Social security number;
- b) Driver’s license number;
- c) California identification number; or
- d) Financial account number, credit or debit card number in combination

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 4.1.2</b>
	<b>Title:</b> <b>INCIDENT RESPONSE PROCEDURE FOR PERSONAL DATA ABOUT CALIFORNIA RESIDENTS</b>	<b>Page: 2 of 9</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/31/03</b>

with required security code, access code, or password that would permit access to an individual's financial account.

Personal information does not include public information that is lawfully made available to the general public from federal, state, and local records.

In the case of any unauthorized intrusion into a server that contains unencrypted personal information, unless specific evidence to the contrary exists, it should be assumed the intruder gained access to the personal information.

An intrusion is defined as unauthorized access to personal information by a person(s) wherein the possibility of use or disclosure for a purpose outside the intended scope of maintaining that information exists.


**B. Roles and Responsibilities**

Responsibility for reporting possible incidents of unauthorized access shall be shared by the local Privacy Officer and the local Information Security Officer, in cooperation with the Incident Response Team. These individuals shall coordinate with the Corporate Privacy/Security Officer to:

- a) Conduct investigations and communicate efforts in the case of an incident;
- b) Notify Divisional and Regional Management of incident;
- c) Notify Regional Counsel of incident;
- d) Notify any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person;
- e) Develop and implement corrective action plans; and
- f) Conduct post-incident evaluations.

**C. Security Breach Assessment**

This guideline assumes that system security measures regarding network, firewall, user accounts, and file security are in place and compliant with Tenet's Information

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 4.1.2</b>
	<b>Title:</b> <b>INCIDENT RESPONSE PROCEDURE FOR PERSONAL DATA ABOUT CALIFORNIA RESIDENTS</b>	<b>Page: 3 of 9</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/31/03</b>

Security Policies and Procedures.

Individuals may become aware of security breaches related to personal information via such methods as system audits and reports by patient(s), physician(s) and others.

Once a potential incident is reported, steps shall be taken to a) verify whether or not an incident has occurred; b) assess the method of intrusion; c) identify the individuals involved in the incident; d) assess the scope of the incident; and e) determine how many individuals may have been impacted by the intrusion. The good faith acquisition of personal information by an employee or agent of Tenet is not a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Each intrusion is unique and next steps will have to be identified after an initial investigation is performed to gather all the facts. Documentation of the results of the investigation shall be maintained. Templates are attached as follows:

- a) Event Chronology Log Form (Addendum A to Incident Response Procedure 4.1.1)
- b) Corrective Action Plan (Addendum B to Incident Response Procedure 4.1.1)
- c) Example Letter to Patient (Addendum A)


D. Notice

Notice must be given to an individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as quickly as possible; provided, however, that such notice may be delayed upon the certification of law enforcement that such notification may impede a criminal investigation. The notice may be in written or electronic form.

**IV. RELATED DOCUMENTS AND REFERENCES:**

This document is directly related to the following documents:

- Incident Response Procedure No. 4.1.1.
- California Senate Bill 1386 (Addendum B).

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 4.1.2</b>
	<b>Title:</b> <b>INCIDENT RESPONSE PROCEDURE FOR PERSONAL DATA ABOUT CALIFORNIA RESIDENTS</b>	<b>Page: 4 of 9</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 12/31/03</b>

- Tips for Victims – Identity Theft – California Dept of Justice  
<http://caag.state.ca.us/idtheft/tips.htm>

**ADDENDUM A**  
**Sample Letter to Patient**

**NOTE:** This letter must be personalized to be specific to each occurrence. The letter should be reviewed by Regional Counsel and the Corporate Privacy/Security Office before it is distributed.

[Organization Letterhead]

Dear *[Patient]*:

I am writing to inform you that a recent incident at our hospital may have exposed you to identity theft. *[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

*[Name of hospital]* is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We suggest that you call 1-800-525-6285 to place a "Fraud Alert" on your credit file with the three major credit bureaus. When you call, you will be prompted by the Equifax voice system to complete the "Fraud Alert" application. This process is fast, easy and free. Putting a "Fraud Alert" on your account will not harm your credit. However it may delay any online ordering or other transactions involving a credit card. You may be asked to provide other personal information to confirm your identity.

When you add a fraud alert to your credit file, you will receive free copies of your credit reports, with toll-free telephone numbers to call if you have any questions about the reports. You should review your reports, and look for accounts you did not open and for inquiries from lenders or creditors that you did not initiate. Check the accuracy of personal information such as home address and Social Security Number (SSN). If you see anything you do not understand, call the credit agency telephone number on the report.

If you find suspicious activity on your credit reports, you may want to contact your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report; creditors may need copies of the report to clear up your records.

Even if you find no signs of fraud on your reports, the California Office of Privacy Protection recommends checking your credit report every three months for the next year.

We deeply regret any inconvenience this incident may cause you, and we assure you that we have implemented additional measures to ensure that your health information is kept safe and secure. If you have additional questions about this incident, you may contact *[Privacy Officer]* at *[Phone Number]*.

*[Closing ]*

**ADDENDUM B**  
**Senate Bill No. 1386**

1798.29.

- (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- (b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- (d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- (e) For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - (1) Social security number.
  - (2) Driver’s license number or California Identification Card number.
  - (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- (f) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- (g) For purposes of this section, “notice” may be provided by one of the following methods:
- (1) Written notice.
  - (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
  - (3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
    - (A) E-mail notice when the agency has an e-mail address for the subject persons.
    - (B) Conspicuous posting of the notice on the agency’s Web site page, if the agency maintains one.
    - (C) Notification to major statewide media. (h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82.

- (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- (d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith

acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

- (e) For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - (1) Social security number.
  - (2) Driver’s license number or California Identification Card number.
  - (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- (f) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- (g) For purposes of this section, “notice” may be provided by one of the following methods:
  - (1) Written notice.
  - (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
  - (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
    - (A) E-mail notice when the person or business has an e-mail address for the subject persons.
    - (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
    - (C) Notification to major statewide media.
- (h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.83.

Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

1798.84.

- (a) Any customer injured by a violation of this title may institute a civil action to recover damages.
- (b) Any business that violates, proposes to violate, or has violated this title may be enjoined.
- (c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.