TRI-CITY HEALTHCARE DISTRICT
AGENDA FOR A REGULAR MEETING
OF THE AUDIT, COMPLIANCE AND ETHICS COMMITTEE
November 17, 2016
8:30 a.m. – 10:30 a.m.
Assembly Rm. 1
Tri-City Medical Center, 4002 Vista Way, Oceanside, CA 92056

The Committee may make recommendations to the Board on any of the items listed below, unless the item is specifically labeled "Informational Only"

	Agenda Item	Time Allotted	Action/ Recommendation	Requestor/ Presenter
1.	Call to order	5 min.		Chair
2.	Approval of Agenda	2 min.		Chair
3.	Public Comments – Announcement Comments may be made at this time by members of the public and Committee members on any item on the Agenda before the Committee's consideration of the item or on any matter within the jurisdiction of the Committee. NOTE: During the Committee's consideration of any Agenda item, members of the public also have the right to address the Committee at that time regarding that item.	1 min.		Standard
4.	Ratification of Minutes- October 20, 2016	3 min.	Action	Chair
5.	New Business – **Discussion and Possible Action**			
	A) **Administrative Policies & Procedures** 1. 8610-292 - Internal Charge Audit	10 min.	Discussion/ Possible Action	C. Thompson
	B) **Compliance Policies** 1. 8610-(NEW) Minimum Necessary Requirements for Use and Disclosure of PHI	10 min.	Discussion/ Possible Action	C. Thompson
	2. 8610-586 - Breach Response	10 min.	Discussion/ Possible Action	C. Thompson
	C) Review of FY2017 1st Quarter Financials	15 min.	Information Only	R. Rivas
6.	Old Business – None			
7.	Motion to go into Closed Session			
8.	Closed Session			
	a. Approval of Audit, Compliance & Ethics Closed Session Minutes of October 20, 2016 (Authority: Government Code Section 54957.2)	5 min.	Approve	Chair
9.	Motion to go into open session			
10.	Open Session			
11.	Report from Chairperson on any action taken in Closed Session (Authority: Government Code, Section 54957.1).	1 min.		

	Agenda Item	Time Allotted	Action/ Recommendation	Requestor/ Presenter
12.	Committee Communications	5 min.		All
13.	Date of Next Meeting January 19, 2017	1 min.		Chair
14.	Adjournment			Chair
15.	Total Time Budgeted for Meeting	1 hour		

Note: Any writings or documents provided to a majority of the members of Tri-City Healthcare District regarding any item on this Agenda will be made available for public inspection in the Administration Department located at 4002 Vista Way, Oceanside, CA 92056 during normal business hours.

Note: If you have a disability, please notify us at 760-940-3347 at least 48 hours prior to the meeting so that we may provide reasonable accommodations

Tri-City Medical Center
Audit, Compliance & Ethics Committee
October 20, 2016
Assembly Room 1
8:30 a.m-10:30 a. m.

Members Present:	Director Ramona Finnila (Chair); Director Larry W. Schallock; Director Laura Mitchell; Jack Cumming, Community Member; Kathryn Fitzwilliam, Community Member; Leslie Schwartz, Community Member; Dr. Cary Mells, Physician Member
Non-Voting Members:	Steve Dietlin (CEO); Ray Rivas, Acting CFO; Kapua Conley, COO; Cheryle Bernard-Shaw, CCO
Others Present:	Diane Racicot, General Counsel; Teri Donnellan, Executive Assistant; Kathy Topp, Director Education & Clinical Informatics

	Discussion	Action Recommendations/ Conclusions	Person(s) Responsible
1. Call to Order	The meeting was called to order at 8:30 a.m. in Assembly Room 1 at Tri-City Medical Center by Chairperson Finnila.		
2. Approval of Agenda	**It was moved by Director Mitchell and seconded by Ms. Kathryn Fitzwilliam to approve the agenda as presented. The motion passed unanimously.**	**Agenda approved.**	Ms. Donnellan
3. Comments by members of the public and committee members on any item of interest to the public before Committee's consideration of the item	There were no public comments.		
4. Ratification of minutes – September 15, 2016	It was noted on page 5 C. the word "laborers" should be revised to read "regulators". **It was moved by Director Schallock and seconded by Director Mitchell to approve the minutes as amended. The motion passed unanimously.**	**Amended Minutes ratified.**	Ms. Donnellan
5. New Business			
A) Review and Discussion of Policies & Procedures:	Director Finnila stated several policies on today's agenda are listed as "deletions". She encouraged committee	**Recommendation to be sent to the Board of**	Ms. Donnellan

	Discussion	Action Recommendations/ Conclusions	Person(s) Responsible
1) 8750-537 – Hiring and Employment; Definitions (DELETE)	members to speak up if they have any questions as to whether information contained in a deleted policy has been addressed elsewhere. Ms. Fitzwilliam stated going forward it would be productive to attach the policies that have the deleted language incorporated to ensure the language has been captured to the committee's satisfaction. Ms. Kathy Topp stated typically the new policy is brought to the committee at the same time as the deleted policy however in this instance that did not occur.	**Directors to delete Policy 8750-537 – Hiring and Employment; Definitions.**	
2) 8750-560 – Responding to Compliance Issues; Introduction; Reports of Suspected Misconduct; Non-Retaliation	The committee had extensive discussion related to Policy 8750-560 – Responding to Compliance Issues; Introduction; Reports of Suspected Misconduct; Non-Retaliation. Suggestions included formatting changes in section A . as well as a modification to the title of the policy. A question was raised regarding whether the District has a Whistle Blower policy. Ms. Bernard-Shaw stated many organizations do not have a specific Whistle Blower Policy as it is counterproductive for the organization, however the policy before the committee today clearly addresses non-retaliation. She stated the purpose of the policy is to be consistent with federal and state law which prohibits retaliation. Ms. Racicot also provided a detailed explanation of the False Claims Act and Deficit Reduction Act. Director Schallock commented on the importance of insuring the Board is informed when those individuals hired by the Board including the CEO, Chief Compliance Officer and General Counsel are being investigated. Ms. Racicot suggested this issue be addressed in Policy 8750-561 as that policy speaks to the process and investigation of suspected misconduct. **It was moved by Ms. Kathryn Fitzwilliam to recommend approval of Policy 8750-561 with amendments as described. Director Mitchell seconded the motion. The**	**Recommendation to be sent to the Board of Directors to Approve Policy**	Ms. Donnellan

4

	motion passed unanimously.	**8750-561 as described.**	
3) 8750-561 – Responding to Compliance Issues – Reports of Suspected Misconduct; Investigation	The committee had extensive discussion on Policy 8750-561 related to how and when the Board is informed of compliance issues related to those individuals hired by the Board (CEO, CCO and General Counsel). Ms. Bernard-Shaw explained the Compliance Officer also makes judgments as to other compliance issues and investigations that should be brought to the attention of the Board. Minor grammatical revisions were also suggested. Ms. Racicot stated in her opinion the policy is not well written and should be tabled to address the issues described.	**Policy 8750-561 – Responding to Compliance Issues – Reports of Suspected Misconduct; Investigation to be revised and brought back to the committee for consideration.**	CCO
4) 8750-563 – Development and Revision of Code of Conduct and Policies – Introduction (DELETE)	Ms. Kathy Topp explained Policy 8750-563 – Development and Revision of Code of Conduct and Policies – Introduction has been deleted and its content has been incorporated into Policy 8750-564.	**Recommendation to be sent to the Board of Directors to delete Policy 8750-563.**	Ms. Donnellan
5) 8750-564 – Development and Revision of Code of Conduct and Policies	The committee reviewed Policy 8750-564 and recommended the following revisions: ➢ Section C. 1. Last line strike the word "Compliance" and replace with the word "Committee". ➢ Section C. 1. Last line insert the words "related compliance" policies, as … ➢ Strike Section D in its entirety. **It was moved by Director Mitchell to recommend approval of Policy 8750-564 – Development and Revision of Code of Conduct and Policies with amendments as described. Mr. Leslie Schwartz seconded the motion. The motion passed unanimously.**	**Recommendation to be sent to the Board of Directors to approve Policy 8750-564 as described.**	Ms. Donnellan
6) 8750-565 – Revision of Conduct and Compliance Policies (DELETE)	It was noted Policy 8750-565 – Revision of Conduct and Compliance Policies has been deleted.	**Recommendation to be sent to the Board of Directors to delete Policy 8750-565.**	Ms. Donnellan
7) 8750-568 – Development and Revision of Code of Conduct and Policies – Dissemination of New or Revised Code of Conduct and Policies (DELETE)	It was noted Policy 8750-568 – Development and Revision of Code of Conduct and Policies – Dissemination of new or Revised Code of Conduct and Policies has been deleted. *Ms. Topp left the meeting at 9:09 a.m.*	**Recommendation to be sent to the Board of Directors to delete Policy 8750-568.**	Ms. Donnellan

B) Consideration to appoint Ms. Kathryn Fitzwilliam to an additional two-year term on the Audit, Compliance & Ethics Committee	**It was moved by Director Schallock to recommend Ms. Kathryn Fitzwilliam be appointed to an additional two-year term on the Audit, Compliance & Ethics Committee. Director Mitchell seconded the motion. The motion passed unanimously.** Chairperson Finnila expressed her appreciation to Ms. Fitzwilliam for her willingness to serve. Chairperson Finnila reported Mr. Barton Sharp's term is also expiring, however he has not expressed an interest in serving an additional term.	**Recommendation to be sent to the Board of Directors to appoint Ms. Kathryn Fitzwilliam to an additional two-year term on the Committee.**	Ms. Donnellan
6. Old Business - None			
7. Oral Announcement of Items to be Discussed during Closed Session (Government Code Section 54957.7)	Chairperson Finnila made an oral announcement of the items listed on the agenda to be discussed during closed session which included approval of closed session minutes.		
8. Motion to go Into closed session	**It was moved by Mr. Jack Cunning and seconded by Director Schallock to go into closed session at 9:10 a.m. The motion passed unanimously.**		
9. Open Session	The committee returned to open session at 9:15 a.m. with attendance as previously noted.		
10. Report from Chairperson on any action taken in Closed Session (Authority: Government Code, Section 54957.1)	Chairperson Finnila reported no action was taken in closed session.		
11. Comments from Committee Members	Director Mitchell expressed her appreciation to Ms. Fitzwilliam for her willingness to serve an additional term.	None	Chairperson
12. Date of Next Meeting	Chairperson Finnila stated the Committee's next meeting is tentatively scheduled for November 17, 2016. Director Schallock commented that the committee should consider cancelling the December 15th meeting due to the Board meeting holiday schedule.	**The committee's next meeting is tentative scheduled November 17, 2016.** **The December 15th meeting will be cancelled.**	
13. Adjournment	Chairperson Finnila adjourned the meeting at 9:15 a.m.		

AUDIT AND COMPLIANCE COMMITTEE
November 17th, 2016

Administrative Policies & Procedures	Policy #	Reason	Recommendations
1. Internal Charge Audit	292	3 year review	
2. Minimum Necessary Requirements for Use and Disclosure of PHI	NEW	NEW	
3. Breach Response	NEW (586)	NEW	

Tri-City Health Care District
Oceanside, California

Administrative Policy Manual
District Operations

ISSUE DATE: 12/10 **SUBJECT: INTERNAL CHARGE AUDIT**

REVISION DATE: **POLICY NUMBER: 8610-292**

Department Approval:	**01/16**
Administrative Policies & Procedures Committee Approval:	~~01/11~~**08/16**
~~**Executive Council Approval:**~~	~~**01/11**~~
~~**Finance & Operations Committee Approval:**~~	~~**01/11**~~
Organizational Compliance Committee Approval:	**10/16**
Audit, Compliance and Ethics Committee Approval:	
Board of Directors Approval:	**01/11**

A. **PURPOSE:**

1. Provide the structure by which the hospital may realize organizational benefits through improvements in internal processes.
2. Improve the provider service relationship by prompt response to patients' billing questions.
3. Identify deficiencies in charge pathways and processes, and strengthen the controls necessary for high-quality fiscal and clinical data.

B. **POLICY:**

1. To ensure all medical billing audits are performed efficiently and effectively, thereby, promoting the accuracy and integrity of hospital charges.

C. **PROCEDURE:**

1. The scope of a medical billing audit is limited to verifying that charges on the detailed hospital bill are accurate, represent services rendered to the patient, and are ordered by a physician. However, services or items may be provided based upon standard hospital practices and/or ~~Nursing~~ **Medical** protocols and procedures.
2. The audit does not assess the "reasonableness" of the charges, or medical necessity related to patient bills. A review of medical necessity for the services provided may be performed, but the billing audit process does not encompass these tasks.
3. Documentation—In concert with the position taken by the American Hospital Association's (AHA) publication, Billing Audit Guidelines (1992), the hospital does not attempt to make the patient's Medical Record a duplicate bill. Rather, the purpose of the Medical Record is to reflect clinical data on diagnosis, treatment, and outcome. Charges on patient bills may be substantiated by ~~Nursing~~ **Medical** protocol and/or standard hospital practices, which are not reflected in the Medical Records. Furthermore, Ancillary departments may have information or documentation not contained in the Medical Record that may be used to substantiate charges. In a business relationship, the hospital will act in good faith during the course of all transactions involving a patient's account, and the same is expected of all outside parties acting on behalf of the patient.
4. ~~HOSPITAL AUDITOR RESPONSIBILITIES~~**Hospital Auditor Responsibilities**:
   a. The hospital will designate an individual to be responsible for coordinating all medical billing audit activities (i.e., Patient Account Auditor; hereafter referred to as Chart Auditor). Medical billing audit activities are prompted via both internal and external processes, and include concurrent, focus, miscellaneous, patient request, and insurance defense audit types. In addition to coordinating all internal audit activities, (i.e., concurrent, focus, and miscellaneous audits), the Chart Auditor will serve as the primary liaison between the hospital and all outside parties requesting patient account audits. All medical billing audit

activities are to be documented and logs maintained within the hospital. All audit-related account adjustments are to be processed only after appropriate facility-level sign off approval has been obtained. All audit related account adjustments are to be signed and dated by the requestor. Principles related to segregation of duties dictate that audit-related account adjustments shall not be processed by the requestor. All audit-related account adjustment documents are to be maintained in accordance with applicable hospital record retention policies.

D. **CONCURRENT ACCOUNT AUDITS INTERNALLY PROMPTED MEDICAL BILLING AUDIT ACTIVITIES**

1. The Chart Auditor will perform concurrent account audits on a monthly basis to identify charge issues that may indicate deficiencies in charge pathways and processes. A concurrent audit is defined as a complete audit of an account completed within 30 days of patient discharge. The audit samples for concurrent review will be determined by the ~~Compliance Committee~~**Senior Director Revenue Cycle~~Integrity, Finance~~**.

~~2. Acute care, psychiatric, and rehabilitation are required to perform additional concurrent account audits. A monthly sample will be determined by the **Senior Director Revenue Integrity, Finance**Compliance Committee.~~

~~3. The Chart Auditor shall be a core member of the Hospital Medical Audit Committee, which is a subcommittee of the Compliance Committee. He/she shall communicate all concurrent audit statistics and identified problems to administrative management within five working days of completion. Concurrent audit summary statistics are to be presented at the monthly meetings of the Hospital Medical Audit Committee.~~

~~4.~~**2.** ~~After review and signature by the Hospital Chief Financial Officer, all concurrent audit statistics, Medical Audit Committee Meeting Minutes, and Departmental Corrective Action Plans are to be sent to the Finance Department by the fifth of each month.~~

~~5.~~**3.** ~~**FOCUS AUDITS**~~**Focus Audits**

a. The Chart Auditor will perform audits on claims chosen to target a specific departmental issue or concern. Focus audits take an in-depth look at very small segments of the hospital's charging structure to make a determination, decision, or conclusion about specific billing or charging practices.

b. Focus audits, which are performed on a select group of claims, may be self-prompted by the Chart Auditor or may come from a committee, group, or entity within the hospital or Tri-City Medical Center. Focus audits are designed to address a variety of issues, including, but not limited to:

   i. Validate or quantify a trend or pattern of billing errors noticed during routine/concurrent audits.
   ii. Complete a quality check on a new service line or new charge capture mechanism.
   iii. Check on the effectiveness of a previously implemented corrective action plan.
   iv. Retrospectively correct accounts in which a specific billing error has been identified.

c. Prior to starting a focus audit, the Chart Auditor must define and document the impetus, approach, timeframe, and extent of the review. This documentation is to be included in the medical billing audit activity logs.

~~d. The Chart Auditor shall communicate all focus audit statistics and identified problems to administrative management within five working days of completion. Focus audit summary statistics are to be presented at the monthly meetings of the Hospital Medical Audit Committee.~~

~~6.~~**4.** ~~MISCELLANEOUS AUDITS~~**Miscellaneous Audits**

a. Internal requests for single account audits from various individuals or departments within the hospital are processed at the discretion of hospital administration. These single account audit requests originate from, but are not limited to, Clinical departments, Business Office, Medical Records, and Finance. ~~A clearly defined internal process for these requests is the responsibility of the Chart Auditor at the direction of hospital~~

~~administration.~~ Documentation of miscellaneous audit activity is recorded and maintained in the medical billing audit activity logs.

b. ~~The Chart Auditor shall communicate all miscellaneous audit statistics and identified problems to administrative management within five working days of completion. Miscellaneous audit summary statistics are to be presented at the monthly meetings of the Hospital Medical Audit Committee.~~

E. EXTERNALLY PROMPTED MEDICAL BILLING AUDIT ACTIVITIES

1. ~~PATIENT REQUEST AUDITS~~**Patient Request Audits**
   a. The hospital will establish and maintain an internal policy for processing patients' questions regarding the validity of itemized charges.
   b. The hospital's Patient Request Audit Policy must address the following issues:
      i. Procedure for referring requests to the Chart Auditor.
      ii. Procedure for communicating audit information to Business Office and Accounts Receivable departments.
      iii. Procedure for communicating audit results to the patient.
      iv. Audit fees (if any).
   c. In the event that a patient's questions can be answered without auditing the bill, notes to that effect must be entered into appropriate hospital files. (i.e., a patient may want to know when or why a particular item or service was provided and has no further billing questions.) If the patient requests a complete bill audit, the following points should be noted:
      i. The entire bill will be audited, not just one department or one section.
      ii. Inform the patient that the bill will be audited for both overcharges and undercharges, and that the claim will be corrected to reflect all billing errors as a result.
      iii. Debits and credits will impact the total charges, but depending on reimbursement methodology, the patient's out-of-pocket expenses may or may not be impacted.
   d. The Chart Auditor shall **provide summary reports for all audits (concurrent, focus, miscellaneous, patient request and third party defense) completed during the month.** ~~**Corrective action plans will be provided by Department Director/Manager with a 5% or greater error rate**communicate all patient request audit statistics and identified problems to administrative management within five working days of completion. Patient request audit summary statistics are to be presented at the monthly meetings of the Hospital Medical Audit Committee~~.

~~F. MEDICAL AUDIT COMMITTEE~~

~~1. Tri-City Medical Center will have a Medical Audit Committee, which is a subcommittee of the Compliance Committee. The purpose of the Medical Audit Committee is to provide a forum for communicating audit results, discussing problematic charge practices, and identifying, initiating, and monitoring corrective actions. The Medical Audit Committee will meet at least nine times annually.~~

~~2. The Medical Audit Committee will include at a minimum: CFO, Director of Patient Business Services, Chart Auditor, HIM director or representative, Nursing director(s), and department directors/managers from Central Supply, Pharmacy, Radiology, Laboratory, and Surgery, as determined necessary by facility. The Medical Audit Committee must be comprised of appropriate representation at a level which ensures problem resolution and decision making.~~

~~3. Department directors/managers are required to attend based on identified error rates:~~
   ~~a. 0 % - 4.99 % error rate: department director/manager is not required to attend Medical Audit Committee meeting~~
   ~~b. 5% or greater error rate: department director/manager attends Medical Audit Committee meeting until all action items are resolved. Director/Manager provides an explanation of the source of errors, how errors may be corrected and presents a detailed corrective action plan addressing root causes; corrective action plans shall include education to prevent recurrence.~~

4. ~~***THE MEDICAL AUDIT COMMITTEE SHALL:***~~

a. ~~Analyze the summarized concurrent audit findings presented by the Medical Billing Auditor. The analysis should:~~

i. ~~Identify departments demonstrating an error rate of greater than 5% in overcharges and undercharges.~~

ii. ~~Discuss possible reasons why overcharges and undercharges are occurring; i.e., failure to properly document services, failure to process credits, failure to accurately capture charges, incomplete documentation on Medication Administration Record, inaccurate charge sheets, lack of departmental charge reconciliation, etc.~~

iii. ~~Discuss corrective action plans. Action plans are designed to assist the departments in moving progressively toward a 0% error rate. Department directors/managers are responsible for establishing control mechanisms to ensure timely, accurate charging and documentation of services rendered.~~

iv. ~~Ensure corrective action plans are implemented no later than 30 days from the date the error rate was identified.~~

v. ~~Monitor and evaluate the effectiveness of all open action plans. Corrective action plans are considered closed when the error rate is below 5% for two consecutive months.~~

b. ~~Analyze the Monthly Late Charge Summary Report. The analysis should:~~

i. ~~Identify departments showing a trend of late charges. Evaluate departments exhibiting late charges greater than 1% of monthly department gross charges.~~

ii. ~~Discuss possible reasons why charges are not processed on a timely basis; i.e., charges not submitted on weekends, failure to batch charges regularly, failure to cross-train personnel on charging practices, incomplete charge information sent to Data Processing, charges generated by the NIC/NMC, lack of departmental reconciliation, etc.~~

iii. ~~Discuss ideas for corrective action by departments exhibiting late charges.~~

iv. ~~Ensure corrective actions are implemented no later than 30 days from the date the late charge rate was reported.~~

v. ~~Monitor and evaluate the effectiveness of all open action items. Corrective actions are considered closed when the applicable department late charge rate is less than 1% for two consecutive months.~~

c. ~~Analyze summarized focus, patient request, miscellaneous, and insurance defense audit findings.~~

5. ~~***MEDICAL AUDIT COMMITTEE DOCUMENTATION***~~

a. ~~The CFO must review and sign all documented Medical Audit Committee activity, which shall include the following:~~

i. ~~Medical Audit Committee meeting agenda and minutes;~~

ii. ~~Signed roster of Medical Audit Committee meeting attendees;~~

iii. ~~Corrective action plans;~~

iv. ~~Summary reports for all audits (concurrent, focus, miscellaneous, patient request and third party defense) completed during the month.~~

6. ~~***REPORTING TO COMPLIANCE COMMITTEE***~~

a. ~~The Medical Audit Committee shall provide monthly reports to the facility's Compliance Committee, including Medical Audit Committee meeting minutes, overall facility error rate trended over 12 months, department error rates trended over 12 months and corrective action plans for any department with an error rate of 10 % or greater. The Compliance Officer or the Compliance Committee shall determine if further audits are required for evaluation and will coordinate this through appropriate channels.~~

7. ~~***ENFORCEMENT***~~

i. ~~All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy.~~

~~Failure to comply with this policy will be subject to appropriate disciplinary action pursuant to all applicable policies and procedures, up to and including termination.~~

Tri-City Medical Center
Oceanside, California

Administrative Policy Manual
Compliance

ISSUE DATE: NEW

SUBJECT: MINIMUM NECESSARY REQUIREMENTS FOR USE AND DISCLOSURE OF PHI

REVISION DATE(S):

POLICY NUMBER:

Department Approval Date(s):	**07/16**
Administrative Policies and Procedures Approval Date(s):	**07/16**
Medical Executive Committee Approval Date(s):	**08/16**
Organizational Compliance Committee Approval Date(s):	**10/16**
Audit, Compliance and Ethics Committee Approval Date(s):	
Board of Directors Approval Date(s):	

A. **PURPOSE:**

1. To establish guidelines for compliance with the Health Insurance Portability and Accountability Act (HIPAA) minimum necessary requirements in order to prevent unlawful or unauthorized access to, and Use and Disclosure of, Protected Health Information.

B. **DEFINITION(S):**

1. **Authorization:** the written form that complies with HIPAA and state law that is obtained from the individual or his or her Personal Representative in order for Tri-City Healthcare District (TCHD) to Use and Disclose Protected Health Information.
2. **Business Associate:** a person or organization who, on behalf of Tri-City Healthcare District (TCHD), performs certain functions or activities involving the Use or Disclosure of PHI or services that require the Business Associate to create, receive, maintain or transmit PHI on behalf of the TCHD or where TCHD needs to Disclose PHI to Business Associates for the services.
3. **Covered Entity:** includes health care providers like the District that transmit health information in electronic form in connection with certain standard transactions (e.g. claims processing).
4. **Disclosure:** the release, transfer, provision of, access to or divulging of PHI outside of TCHD.
5. **Electronic Protected Health Information (EPHI):** PHI that is transmitted by Electronic Media or Maintained in Electronic Media.
6. **Individual:** the person who is the subject of protected health information.
7. **Minimum Necessary:** refers to TCHD or a business associate taking reasonable efforts to Use, Disclose, and ~~r~~Request only the minimum amount of protected health information needed to accomplish the purpose.
8. **Protected Health Information (PHI):** individually identifiable health information transmitted or maintained in paper or electronic form that is created or received by TCHD AND
   a. Relates to the past, present, or future physical or mental health or condition of an individual; OR
   b. Relates to the provision of health care to an individual; OR
   c. Relates to the past, present, or future payment, AND
   d. Identifies the individual OR with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
9. **Use:** the sharing, application, utilization, examination or analysis of PHI within TCHD.
10. **Workforce:** employees, volunteers, trainees, and other persons whose conduct, in the performance of work for TCHD is under the direct control of TCHD whether or not they are paid by TCHD.

C. **POLICY:**

1. Unless an exception applies, Uses and Disclosures of PHI, and requests to other Covered Entities for PHI, shall be limited to the amount of information reasonably necessary to accomplish the purpose of the Use, Disclosure or rRequest.
2. TCHD shall identify levels of access, review, or viewing of patient medical information by Workforce members in order to comply with state and federal privacy laws.
3. TCHD may not Use, Disclose or rRequest an entire medical record unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the Use, Disclosure or rRequest.
4. The minimum necessary requirements do not apply in the following circumstances:
   a. Disclosures made or requests by a health care provider for treatment purposes;
   b. Disclosures to the patient who is the subject of the information;
   c. Uses or Disclosures made pursuant to an Individual's Authorization;
   d. Disclosures to the Department of Health and Human Services when Disclosure is required under HIPAA;
   e. Uses or Disclosures required by law; and
   f. Uses or Disclosures required for compliance with HIPAA.

D. **PROCEDURE:**

1. Uses: Identification of Workforce member Use of PHI for job duties.
   a. TCHD shall identify persons or classes of persons within TCHD's Workforce who need access to PHI to carry out their job duties, the PHI or types of PHI needed and conditions of such access.
   b. Each TCHD Department is responsible for making reasonable efforts to limit access to PHI to that necessary to carry out the job duties, functions and/or responsibilities. Role based access relates to both hard copy and electronic medium. [Attachment A identifies the PHI access standards for TCHD Workforce members.]
   c. Employee access to their own medical record requires submission of a written request/consent submitted to the Medical Records/Health Information department where a copy or CD of the information requested will be provided.
   d. Questions regarding the minimum necessary requirements should be directed to the Department Supervisor, Privacy Officer or HIPAA Security Officer.
2. Disclosures: TCHD's Disclosures of PHI in response to requests from other parties.
   a. For any Disclosure of PHI made on a routine or recurring basis, TCHD must limit the PHI Disclosed to the amount reasonably necessary to achieve the purpose of the Disclosure. Individual review of each routine or recurring Disclosure is not required. [Attachment B establishes procedures designed to limit the PHI Disclosed by TCHD to the amount reasonably necessary to achieve the purpose of the Disclosure.]
   b. For all non-routine/non-recurring Disclosures, TCHD must review the Disclosure on an individual basis in accordance with the criteria set forth in Attachment B.
   c. In certain circumstances, TCHD may (but is not required to) reasonably rely on the judgment of the party who is requesting Disclosure in determining the amount of information that is needed. Reliance is permitted when it is reasonable under the particular circumstances and when the request for Disclosure is made by:
      i. A public official or agency that states that the information requested is the minimum necessary for a permitted purpose under HIPAA (e.g. public health purposes);
      ii. Another Covered Entity;
      iii. A professional who is a TCHD Workforce member or Business Associate who represents that the information requested from TCHD is the minimum necessary and who makes the request in order to provide professional services to TCHD; and
      iv. A researcher with documentation from an Institutional Review Board that complies with 45 CFR Section 164.512(i).
3. Requests: TCHD's requests to other parties for PHI.

a. For any request of PHI made to another Covered Entity, TCHD must limit such request to the PHI which is reasonably necessary to accomplish the purpose for which the PHI is requested.
b. For any request of PHI made on a routine or recurring basis, TCHD must limit the PHI to that which is reasonably necessary to accomplish the purpose for which the PHI was requested. Individual review of each routine or recurring request for PHI is not required. [Attachment C identifies procedures designed to limit the PHI requested by TCHD to the amount reasonably necessary to achieve the purpose of the request.]
c. For all non-routine/non-recurring requests for PHI, TCHD must review the Disclosure on an individual basis in accordance with the criteria set forth in Attachment C.

4. Minimum Necessary Requirements Not Applicable:
   a. The minimum necessary requirements do not apply to the following Uses and Disclosures of PHI and/or request for PHI:
      i. Disclosures made or request by a health care provider for treatment purposes;
      ii. Disclosures to the patient who is the subject of the information;
      iii. Uses or Disclosures made pursuant to an Individual's Authorization;
      iv. Disclosures to the Department of Health and Human Services when Disclosure is required under HIPAA;
      v. Uses or Disclosures required by law; and
      vi. Uses or Disclosures required for compliance with HIPAA.

E. **RELATED DOCUMENT(S):**
1. Attachment A - PHI Access Rights for TCHD Workforce Members
2. Attachment B – TCHD Disclosures of PHI
3. Attachment C – TCHD Requests for PHI to Third Parties

F. **REFERENCES:**
1. 45 CFR Section 160.103
2. 45 CFR Section 164.502(b)
3. 45 CFR Section 164.512(i)
4. 45 CFR Section 164.514(d)
5. California Civil Code 56 et seq.
6. California Health & Safety Code Section 1280.15

ATTACHMENT A
PHI ACCESS RIGHTS FOR TCHD WORKFORCE MEMBERS

Job Title/Category	Description of Permitted PHI Access	Conditions
Attending Physician	All System Components	Provider-Patient Relationship /Need-to- know
Admitting/Registration	Limited to patient demographics, eligibility, and administrative documents	Need-to-know
Business Development	**Evaluation of business programs and required quarterly metrics**	**Need-to-know**
Clinical Research	As specified in patient authorization, IRB documentation or data use agreement consistent with 45 CFR 164.512(i)	Research patient only
Coding and Abstracting	Access HIM utilized when coding/abstracting encounters for billing and/or data collection.	Need-to-know
Compliance office	Audits, reviews or investigations	As CCO determines necessary for audits, reviews or investigations.
Cardiology Services	Results of cardiac related tests and procedures performed Powerchart – Nursing module Registration module Laboratory module Diagnostic Imaging module	Need-to-know
Environmental Services	Limited – bed turnover	Need-to-know
Facilities Department	NONE	Not applicable
Finance	Limited - Coded information (DRGs, APR-DRGs, etc.)	To support analysis of patient activity, ~~and~~ facility programs **and complete accounts payable**
Home Health	**Home Care/Home Base application in addition to Powerchart discharge information**	**Patient Care relationship – Need to know**
Imaging / Radiology	Powerchart – Nursing module Registration/Scheduling module Laboratory module Diagnostic Imaging module RadNet, PACs system images and results, Powerchart, FirstNet	Need-to-know
Laboratory	Powerchart – Nursing module Registration/Scheduling module Laboratory module - PathNet Diagnostic Imaging module RadNet, PACs system images and results, Powerchart, FirstNet	Need-to-know
Leadership	**Powerchart for review of quality measures as well as audits to confirm documentation practices are compliant with regulations.**	**Minimum necessary to meet the intent of the audit/chart review.**
Marketing	As specified in patient authorization	Written consent required by patient/patient rep.

Materials	**Limited – as needed to manage ordering, recalls and purchasing**	**Need-to-know, Recall Follow-up**
Medical Records/HIM	Release of Information to Clinics, MD Offices, and external care providers. Respond to Quality reviews and RAC related requests.	Minimum necessary to meet needs or request
Nutrition Services	**Powerchart – Nursing module** **Laboratory module** **Diagnostic Imaging module** **FirstNet, SurgiNet**	**Patient Care Relationship** **Need-to-know**
Privacy Officer	Privacy Officer Audits and Investigations	To support review of appropriate access, use and disclosure by user.
Patient Accounting	All billing and collection activities to include Denials Management, credit balances,	Specific documentation to support the appeal of a denial.
Patient Accounts Rep	Registration module Patient Accounts module Coding and Abstracting module	Need-to-know
Patient Care Services	**Powerchart – Nursing module** **Registration module** **Laboratory module** **Diagnostic Imaging module** **FirstNet, SurgiNet**	**Patient Care Relationship** **Need-to-Know**
Pharmacist	PharmNet and PowerChart Laboratory module	Need-to-know
Pharmacy Technician	Powerchart – Nursing module Laboratory module	Need to know
Physical Therapist	Powerchart – Nursing module Registration module Laboratory module Diagnostic Imaging module	Patient Care relationship Need-to-know
~~Registered Nurse~~	~~Powerchart – Nursing module~~ ~~Registration module~~ ~~Laboratory module~~ ~~Diagnostic Imaging module~~	~~Patient Care Relationship~~ ~~Need-to-Know~~
Risk, Regulatory Services **and Quality**	Powerchart for review of quality measures as well as audits to confirm documentation practices are compliant with regulations.	Minimum necessary to meet the intent of the audit/chart review.
Respiratory Therapist	Powerchart – Nursing module Registration module Laboratory module Diagnostic Imaging module	Patient Care relationship Need-to-know
Surgical Services	Surgi-Net system for documentation of details relating to surgical procedures Powerchart – Nursing module Registration module Laboratory module Diagnostic Imaging module	Patient Care relationship Need to know
Utilization Management	Entire patient record for treatment and operations. Use of record to support appeals relating to denied days/stays.	Patient Care relationship. Need to know.

*** Not a comprehensive list**

ATTACHMENT B
TCHD DISCLOSURES OF PHI

1. TCHD will be responsible for reviewing requests for Disclosure of PHI to determine whether the minimum necessary requirements apply and, if they apply, to determine what amount of information is appropriate for Disclosure.
2. Once TCHD makes a determination on a particular request, if the type of request becomes routine or recurring, TCHD does not have to review all subsequent requests on an individual basis. This assumes, however, that appropriate steps are taken to limit the Disclosures to the minimum necessary to accomplish the purpose as provided in these guidelines.
3. If the request **IS** made for the purpose of Treatment of a patient by another health care provider, the minimum necessary requirements **do not apply**, and the PHI that is requested may be released.
4. If the request **IS NOT** made for the purposes of Treatment of a patient **BUT** an exception to the minimum necessary requirements applies, TCHD may release the PHI provided that TCHD has authority to disclose the requested PHI under state and federal privacy laws.
5. If the request **IS NOT** made for purposes of Treatment **AND** the minimum necessary standards do apply, then TCHD must:
   a. Confirm that Disclosure of the PHI requested is permitted under applicable federal and state privacy laws.
   b. If the Disclosure of PHI is otherwise permitted under applicable federal and state privacy laws, review the request for the purpose and release only the minimum amount of information necessary to meet the purpose of the request.
   c. If the request does not indicate a purpose, determine whether it is possible to obtain a revised request or a verbal statement of the purpose which should be documented. Once the third party furnishes a description of the purpose, take appropriate action to provide the minimum amount of information necessary to meet the purpose of the request.
   d. The Privacy Officer should be consulted if there are any questions regarding a request for PHI including those circumstances where TCHD intends to rely on the judgment of the party making the request for PHI that the amount of PHI requested is the minimum necessary for the purpose for which it was requested.
   e. The Privacy Officer may also consult with the Chief Compliance Officer and/or legal counsel as necessary and appropriate to respond to Disclosure requests.
6. For Routine or Recurring Disclosures of PHI, TCHD shall Disclose as follows:

Recipient	Purpose	Minimum Necessary
Ambulance Company	Obtain demographic and insurance information for billing	Facesheet or data transfer with patient demographics and insurance information
Attorney	Evaluate individual's medical condition in support of a lawsuit	Specific information request
Collection Agency	Obtain payment on past due accounts	File of patient names, addresses, dates of service and amount owed
Contracted Payor	Validation of services and DRG assignment	Specific medical data under review
Law Enforcement (Police)	Investigation	Review/Evaluate written request to confirm minimum necessary provided to meet elements of the request.
Physician	Administrative oversight ((i.e. Medical Director, Institute operations)	Summary patient information for monitoring program

Iron Mountain	Record retention	All records to be stored
Quality Improvement Organizations	Healthcare operations	Specific medical data under review
Recovery Audit Contractor	Minimum necessary to meet needs or request	Specific medical data under review
Shredding s**S**ervice	Record Disposal/Destruction	All records as described in the Services Agreement and BAA

7. For non-routine Disclosures of PHI, TCHD must review them on a case-by-case basis in accordance with the criteria set forth above.
   a. Patient Request for Continuing Care
   b. Legal Review (internal)
   c. Subpoena

ATTACHMENT C
TCHD REQUESTS FOR PHI TO THIRD PARTIES

1. TCHD will be responsible for reviewing requests for Disclosure of PHI made to other Covered Entities to determine whether the minimum necessary requirements apply and, if they apply, to determine what amount of information is appropriate for Disclosure.
2. Once TCHD makes a determination on a particular request, if the type of request becomes routine or recurring, TCHD does not have to review all subsequent requests on an individual basis. This assumes, however, that appropriate steps are taken to limit the requests to the minimum necessary to accomplish the purpose as provided in these guidelines.
3. If the request for PHI IS MADE for the purpose of Treatment of a patient, the minimum necessary requirements do not apply.
4. If the request IS NOT made for purposes of Treatment AND the minimum necessary standards do apply, then TCHD must:
    a. Request only the minimum necessary to accomplish the purpose for which the request is made.
    b. Provide the purpose of the PHI when requesting PHI from other Covered Entities.
    c. The Privacy Officer should be consulted if there are any questions regarding a request for PHI including where TCHD intends to rely on the judgment of the party making the request for PHI that the amount of PHI requested is the minimum necessary for the purpose for which it was requested.
    d. The Privacy Officer may also consult with the Chief Compliance Officer and/or legal counsel as necessary and appropriate to respond to Disclosure requests.
5. For Routine or Recurring requests for PHI, TCHD shall request PHI as follows:

Request	Purpose	Minimum Necessary
Example: **Physician**	**Healthcare operations: Quality review**	**Specific medical data under review**
Healthcare Facilities	**Healthcare operations**	**PHI to provide continuing care**

6. For non-routine requests for PHI, TCHD must review them on a case-by-case basis in accordance with the criteria set forth above.

Tri-City Medical Center
Oceanside, California

Administrative Policy Manual
Compliance

ISSUE DATE: NEW **SUBJECT:** BREACH RESPONSE

REVISION DATE(S): **POLICY NUMBER:** 8610-586

Department Approval Date(s):	**06/16**
Administrative Policies and Procedures Approval Date(s):	**07/16**
Medical Executive Committee Approval Date(s):	**08/16**
Organizational Compliance Committee Approval Date(s):	**10/16**
Audit, Compliance and Ethics Committee Approval Date(s):	
Board of Directors Approval Date(s):	

A. **PURPOSE:**

1. To outline the steps that must be taken by Tri-City Healthcare District (TCHD) to investigate and confirm a Breach and/or unlawful or Unauthorized Access to PHI and the requirements for notification of such Breach and/or unlawful or Unauthorized Access to PHI to affected patients and to Federal and/or State regulators.

B. **DEFINITION(S):**

1. **Breach:** an impermissible acquisition, access, Use or Disclosure of Protected Health Information under the Privacy Rule that compromises the security or privacy of the Protected Health Information.
2. **Business Associate:** a person or organization who, on behalf of the District, performs certain functions or activities or services that require the Business Associate to create, receive, maintain, or transmit PHI on behalf of the District or where the District needs to disclose PHI to a Business Associate for the services.
3. **California Department of Public Health (CDPH):** The Department of the State of California to which reports required by Health & Safety Code Section 1280.15 are made.
4. **Disclosure:** the release, transfer, provision of, access to or divulging of PHI outside of TCHD.
5. **Electronic Protected Health Information (EPHI):** Individually identifiable health information that is transmitted by electronic media or maintained in electronic media.
6. **Office of Civil Rights (OCR):** The federal entity to which Breach reports required under HIPAA are made.
7. **Protected Health Information (PHI):** individually identifiable health information transmitted or maintained in paper or electronic other form that is created or received by TCHD AND
   a. Relates to the past, present, or future physical or mental health or condition of an individual; OR
   b. Relates to the provision of health care to an individual; OR
   c. Relates to the past, present, or future payment AND
   d. Identifies the individual OR with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
8. **Security Incident:** attempted or successful unauthorized access, Use or Disclosure, modification or destruction of information or interference with systems operation in an information system.
9. **Unauthorized Access:** as provided under Health & Safety Code Section 1280.15, the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the California Confidentiality of Medical Information Act or any other statute or regulation governing the lawful access, use, or disclosure of medical information.

10. **Unsecured PHI:** PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of the Department of Health and Human Services.
11. **Use:** the sharing, application, utilization, examination or analysis of PHI within TCHD.

C. **POLICY:**

1. It is the policy of TCHD to review and investigate each report or other discovery of a potential Breach or unlawful or Unauthorized Access to a patient's PHI in order to assess and confirm whether such events have occurred and whether notice to patients and reporting to regulators is required.
2. It is the policy of TCHD to provide notice to affected patients of an identified Breach of Unsecured PHI and/or unlawful or Unauthorized Access to PHI and to report such matters to the CDPH, the OCR and/or the Office of the California Office of the Attorney General if an as required by law and this Policy.
3. TCHD's Privacy Officer is responsible for investigating suspected or actual Breaches and/or any unlawful or Unauthorized Access to PHI and for coordinating notices to patients and reports to regulators. TCHD's Security Officer is responsible for working with the Privacy Officer to investigate suspected Breaches involving EPHI, including those that arise from Security Incidents.

D. **PROCEDURE:**

1. Internal Breach Reporting: The following steps must be taken when there is a suspected or known known Breach and/or unlawful or Unauthorized Access of PHI:
   a. Board Members, Employees, interns, physicians, and Business Associates are required to immediately report a suspected or known Breach and/or unlawful or Unauthorized Access of PHI. Notification can be accomplished through notification to their direct supervisor or to a Director, Privacy Officer, Security Officer, or via the confidential reporting line (ValuesLine).
   b. Breach Response Team notified of reported Breach and/or unlawful or Unauthorized Access events.
   c. Review and evaluation of the Breach report is completed with leadership representatives (i.e. CEO, COO, CFO, CNE, Privacy Officer, HIPAA Security Officer, Director of Regulatory services, etc.) in the areas in which the Breach and/or unlawful or Unauthorized Access occurred to determine the:
      i. Included Patient identifiers;
      ii. Method of the suspected or actual Breach and/or unlawful or Unauthorized Access;
      iii. Individual(s) involved in the suspected or actual Breach and/or unlawful or Unauthorized Access;
      iv. Volume of patients impacted;
      v. Whether the volume of patients impacted triggers additional notifications (i.e. less than 500 patients involved vs. 500 or more patients involved);
      vi. Whether the suspected Breach involves Unsecured PHI and/or constitutes unlawful or Unauthorized Access to PHI which must be reported to patients, regulators and/or the media under HIPAA and/or state laws; and
      vii. Information that may be used to mitigate potential harm to patients (e.g. return/recovery of PHI, erasure of EPHI from lost or stolen devices, etc.).
      viii. Breach activity is reported to the Organizational Compliance Committee and the Audit Compliance and Ethics (ACE) Committee of the Board.
2. Breach Reporting by Business Associates:
   a. Business Associates are required to notify TCHD Privacy Officer of Breaches of Unsecured PHI and/or unlawful or Unauthorized Access to PHI without unreasonable delay and no later than 24 hours from the date of the potential/actual Breach.
   b. To the extent possible, Business Associates should provide TCHD with the identification of each individual affected and identifiers, the date of the Breach or unlawful or

Unauthorized Access, as well as any other available information required to be provided by TCHD in the notification to affected individuals or to regulators.

c. Review and evaluation of the Breach report is completed with leadership representatives (i.e. CEO, COO, CFO, CNE, Privacy Officer, HIPAA Security Officer, Director of Regulatory services, etc.) in the areas in which the suspected or actual Breach and/or unlawful or Unauthorized Access occurred to determine:
   i. Included Patient identifiers;
   ii. Method of the suspected or actual Breach and/or unlawful or Unauthorized Access;
   iii. Individual(s) involved in the suspected or actual Breach and/or unlawful or Unauthorized Access;
   iv. Whether the suspected or actual Breach involves Unsecured PHI and/or otherwise constitutes unlawful or Unauthorized Access to PHI which must be reported to patients, regulators and/or the media under HIPAA and/or state laws;
   v. Volume of patients impacted; and
   vi. Whether the volume of patients impacted triggers additional notifications (i.e. less than 500 patients involved vs. 500 or more patients involved); and
   vii. Information that may be used to mitigate potential harm to patients (e.g. return/recovery of PHI, erasure of EPHI from lost or stolen devices, etc.).

3. Breach Response:
   a. Breaches or Unlawful or Unauthorized Access Related to PHI – Privacy:
      i. Incident/Breach is reported to the Facility's Privacy Officer. Details relating to the issue are confirmed in writing by the area/department involved in the suspected or actual Breach or unlawful Unauthorized Access. Information includes:
         1) Date/Time of the events.
         2) Patient/Patient's involved in the events (unauthorized disclosure).
            a) Confirmation of the PHI elements involved.
         3) Identification of the individual(s) (e.g. staff member(s), business associates) involved in actions that resulted in the suspected or actual Breach or unlawful or Unauthorized Access.
         4) Confirmation of steps taken to mitigate the confirmed Breach or unlawful or Unauthorized Access, including any identified Security Incident that results in a Breach of Unsecured PHI.
         5) Notification Date/Time of Privacy Officer.
   b. Breaches or Unlawful or Unauthorized Access Related to EPHI – Security:
      i. Security Incident or other suspected or actual Breach, unlawful or Unauthorized Access (including Security Incidents) related to EPHI is reported to TCHD's HIPAA Security Officer. Details relating to the event are evaluated and documented to include:
         1) Dates/Times when the event occurred/was discovered
         2) Current Date/Time
         3) Name of Individual(s) who discovered the Breach or Unlawful or Unauthorized Access
         4) To whom was the breach reported;
         5) Date/Time Breach Response Team notified
         6) Confirm whether and to what extent systems and data exposed, accessed or destroyed, if any
            a) What system(s) is affected
            b) What type of breach occurred
            c) What was stolen
            d) Who all is aware of the breach
         7) Secure the premises and information systems locations as appropriate.
         8) Determine immediate actions that need to be taken to secure information systems and EPHI (e.g. take the affected server, application, etc. off-line, wipe portable devices, etc.)

9) Interview those persons involved in discovering the suspected Breach or unlawful or Unauthorized Access and others who may have knowledge.
10) Confirm need to engage a forensics team to assist in review.

c. Consult with Legal Counsel, as necessary and appropriate.

4. Breach Notifications
   a. Following a Breach of Unsecured PHI, TCHD will provide notification of the Breach of Unsecured PHI or unlawful or Unauthorized Access to PHI to:
      i. Affected individual(s) (by the Privacy Officer)
         1) Notification is provided via first class mail or e-mail (if the patient has requested to received information in this manner).
         2) Notice must be provided within 15 days.
      ii. CDPH
         1) Upon receipt of communication relating to a Breach of Unsecured PHI and/or unlawful or Unauthorized Access to PHI, the Director, Regulatory Services will notify the ~~California Department of Health (~~CDP**H**~~J)~~ via phone call within 5 days with follow-up with written notification submitted within 15 days of knowledge of the breach.
         2) The Regulatory Director tracks the breach information to the Professional Affairs Committee.
            a) Individual breach reporting posted by March 31st annually.
            b) Breach of Unsecure PHI volumes greater than 500 are reported within 30 days of the breach.
         3) Name of individual(s) involved in the Breach of Unsecure PHI or unlawful or Unauthorized Access to PHI.
         4) Notice must be provided within 15 days.
      iii. Office of Civil Rights
         1) To be notified on an annual basis (submission required by March 1st).
   b. To the extent possible, Business Associates should provide TCHD with the identification of each individual affected and identifiers included in the Breach, the date of the Breach, as well as any other available information required to be provided by TCHD in the notification to affected individuals or to regulators.

5. Additional Requirements for a Breach where 500 or more individuals are affected:
   a. Legal Counsel notified of the Breach;
   b. Determine resources to support of required steps e.g. notifications (preparation, review and distribution), mitigation (e.g. credit report monitoring, IT staff, etc.).
   c. Media Notice/statement generated to (for 90 days). ~~:~~
   d. TCHD will set up a **toll-free** call center ~~(1-800 number~~ to be available for patients to call with questions~~)~~**.**
   e. Secretary, Office of Civil Rights is notified without delay and in no case later than 60 days following the Breach.
   f. Consult and coordinate notice to local media**.**
   g. Determine appropriate notifications to be posted on TCHD Web-site including distribution of ~~1-800~~**the toll-free** number.
   h. For Breaches of unencrypted computerized data that includes personal information, determine whether notice must be given to patients and a copy of the data breach notice (without personal information) must be provided to the California Office of the Attorney General pursuant to California Civil Code sections 1798.29 and 1798.82.

6. Notifications to Insurance Carrier:
   a. TCHD's Privacy Officer shall consult with TCHD Finance and/or Risk Management to determine if notice needs to be provided to any insurance carrier providing coverage for privacy, security and/or cybersecurity incidents.

7. HIPAA Breach Exceptions:
   a. The following scenarios constitute exclusions from Breaches under HIPAA:
      i. Unintentional acquisition, access, or Use of PHI by:

1) A workforce member, or person acting under the authority of TCHD or a TCHD Business Associate, if such acquisition, access, or use was made in good faith and within the user's scope of authority and does not result in a further Use of Disclosure that is not permitted under HIPAA.

ii. Inadvertent Disclosure of PHI:

1) By persons authorized to access PHI at TCHD; or by a TCHD Business Associate to another person authorized to access PHI at TCHD or TCHD Business Associate; or to an organized healthcare arrangement in which TCHD participates. Information received as a result of such Disclosure cannot be further Used or Disclosed in a manner not permitted by HIPAA.

iii. A Disclosure of PHI where TCHD or TCHD Business Associate has a good faith belief that the unauthorized person to whom the impermissible Disclosure was made would not reasonably have been able to retain the information.

8. Burden of Proof:

a. TCHD is required to demonstrate that all required notifications have been provided or that the Use or Disclosure of Unsecured Protected Health Information did not constitute a Breach. A Breach of PHI is presumed unless TCHD or a Business Associate demonstrates there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

b. Breach of Unsecured PHI/Unlawful or Unauthorized Access:

i. TCHD shall maintain documentation that all required notifications were made and for the time required in TCHD Policy.

c. When a determination has been made that a Breach did not occur and notification is not required the following documentation is maintained:

i. Assessment demonstrating a low probability that the PHI has been compromised by the Impermissible Use or Disclosure; and

ii. The applicability of any other exceptions to the definition of Breach.

9. Distribution of Breach Guidance

a. TCHD workforce members are educated on the process for reporting and notification of a suspected or actual Breach or unlawful or Authorized Access of PHI upon hire and annually.

b. TCHD Business Associates are required to follow the requirements for handling suspected or actual Breaches or unlawful or Authorized Access of PHI set forth in their Business Associate Agreement.

E. REFERENCE LIST:

1. California Health & Safety Code §1280.15
2. California Civil Code Sections 1798.29 and 1798.82
3. 45 Code of Federal Regulations (CFR) §164.402
4. 45 CFR §164.404
5. 45 CFR §164.406
6. 45 CFR §164.408