

AGENDA
CORPORATE COMPLIANCE/PRIVACY AND INTERNAL AUDIT
COMMITTEE MEETING OF THE EL CAMINO HOSPITAL BOARD

Thursday, May 18, 2017 – 5:00 pm

El Camino Hospital, Conference Room F (ground floor)
2500 Grant Road, Mountain View, CA 94040

Lica Hartman will be participating via teleconference from 5400 Computer Dr. Westborough, MA 01581.

Dennis Chiu will be participating via teleconference from 185 Greenwood Drive, Napa, CA 94558.

PURPOSE: The Corporate Compliance/Privacy and Internal Audit Committee is responsible for providing direction for both the Corporate Compliance and Internal Audit programs at all locations of El Camino Hospital (ECH). Responsibilities include providing oversight on compliance issues requiring executive-level interaction, assessing physician relationship risk as it relates to compliance, reviewing HIPAA/Privacy laws as they relate to compliance, and directing ECH on compliance strategies. The Committee also serves as the ad-hoc mobilization team for any external investigations and/or actions. Further, additional responsibilities include providing direction and oversight to ongoing internal audit activity and determining appropriate organizational response in order to identify and mitigate organizational risk.

AGENDA ITEM	PRESENTED BY		ESTIMATED TIMES
1. CALL TO ORDER / ROLL CALL	John Zoglin, Chair		5:00 – 5:01 pm
2. POTENTIAL CONFLICT OF INTEREST DISCLOSURES	John Zoglin, Chair		5:01 – 5:02
3. PUBLIC COMMUNICATION a. Oral Comments <i>This opportunity is provided for persons in the audience to make a brief statement on issues or concerns not covered by the agenda.</i> b. Written Correspondence	John Zoglin, Chair		information 5:02 – 5:05
4. CONSENT CALENDAR <i>Any Committee Member or member of the public may remove an item for discussion before a motion is made.</i> Approval a. Minutes of the Open Session of the Corporate Compliance/Privacy and Internal Audit Committee Meeting (March 16, 2017) Information b. Status of FY17 Committee Goals	John Zoglin, Chair	<i>public comment</i>	motion required 5:05 – 5:10
5. REPORT ON BOARD ACTIONS ATTACHMENT 5	John Zoglin, Chair		information 5:10 – 5:15
6. POLICIES FOR APPROVAL a. Information Security: 1.04 Network Access Control b. Information Security: 1.02 Authorized Access to Information Systems c. Information Security: 0.01 Information Security Management Program d. Information Security: 1.01 Business Requirement for Access Control e. Information Security: 1.03 User Responsibilities f. Corporate Compliance: 51.00 Physician Financial Arrangements – Review and Approval ATTACHMENT 6	Diane Wigglesworth, Sr. Director, Corporate Compliance	<i>public comment</i>	possible motion 5:15 – 5:20

A copy of the agenda for the Regular Committee Meeting will be posted and distributed at least seventy-two (72) hours prior to the meeting. In observance of the Americans with Disabilities Act, please notify us at (650) 988-7504 prior to the meeting so that we may provide the agenda in alternative formats or make disability-related modifications and accommodations.

AGENDA ITEM	PRESENTED BY		ESTIMATED TIMES
7. REVIEW PROPOSED FY18 COMMITTEE GOALS ATTACHMENT 7	Diane Wigglesworth, Sr. Director, Corporate Compliance	<i>public comment</i>	motion required 5:20 – 5:25
8. REVIEW PROPOSED FY17 FINANCIAL AUDIT PLAN ATTACHMENT 8	Brian Conner, Moss Adams		information 5:25 – 5:35
9. HIMSS CONFERENCE: COMPLIANCE RISKS AND IT SECURITY HIGHLIGHTS ATTACHMENT 9	Diane Wigglesworth, Sr. Director, Corporate Compliance		information 5:35 – 5:45
10. KEY PERFORMANCE INDICATORS, SCORECARD AND TRENDS ATTACHMENT 10	Diane Wigglesworth, Sr. Director Corporate Compliance		information 5:45 – 5:50
11. ADJOURN TO CLOSED SESSION	John Zoglin, Chair		motion required 5:50 – 5:51
12. POTENTIAL CONFLICT OF INTEREST DISCLOSURES	John Zoglin, Chair		5:51 – 5:52
13. CONSENT CALENDAR <i>Any Committee Member may remove an item for discussion before a motion is made.</i> Approval <i>Gov't Code Section 54957.2</i> a. Minutes of the Closed Session of the Corporate Compliance/Privacy and Internal Audit Committee Meeting (March 16, 2017) Information <i>Gov't Code Section 54956(d)(2) – Conference with legal counsel – pending or threatened litigation.</i> b. Compliance Log (March-April 2017) c. Privacy Log (March-April 2017) d. Internal Audit Follow Up e. Internal Audit Work Plan f. Pacing Plan	John Zoglin, Chair		motion required 5:52– 5:54
14. Report involving <i>Gov't Code Section 54956(d)(2) – Conference with legal counsel – pending or threatened litigation:</i> - Report on Internal Audit Assessment and Work Plan	Alex Robison, Protiviti		motion required 5:54 – 6:04
15. Report involving <i>Gov't Code Section 54956(d)(2) – Conference with legal counsel – pending or threatened litigation:</i> - Report on Internal Audit Activity	Diane Wigglesworth, Sr. Director Corporate Compliance		information 6:04 – 6:14
16. <i>Health and Safety Code Section 32106(b)</i> for a report involving health care facility trade secrets: - Discussion on ERM Reporting	Mick Zdeblick, COO		possible motion 6:14 – 6:34

AGENDA ITEM	PRESENTED BY		ESTIMATED TIMES
17. Discussion involving <i>Gov't Code Section 54956(d)(2)</i> – Conference with legal counsel – pending or threatened litigation: - Discussion on IT Security	Deb Muro, Interim CIO		possible motion 6:34 – 6:54
18. Report involving <i>Gov't Code Section 54957</i> for discussion and report on personnel performance matters: - Executive Session	John Zoglin, Chair		discussion 6:54 – 6:57
19. ADJOURN TO OPEN SESSION	John Zoglin, Chair		motion required 6:57 – 6:58
20. RECONVENE OPEN SESSION / REPORT OUT To report any required disclosures regarding permissible actions taken during Closed Session.	John Zoglin, Chair		6:58 – 6:59
21. ADJOURNMENT	John Zoglin, Chair		motion required 6:59 – 7:00pm

Upcoming Meetings

- June 14, 2017 (*Joint Session with Hospital Board*)

 (*tentative upon Committee and Board approval*)
- August 17, 2017
- September 28, 2017
- November 16, 2017
- January 18, 2018
- March 15, 2018
- May 17, 2018



**Minutes of the Open Session of the
Corporate Compliance/Privacy and Internal Audit Committee
Thursday, March 16, 2017
El Camino Hospital | Conference Room F
2500 Grant Road, Mountain View, CA 94040**

Members Present

John Zoglin, Chair
Sharon Anolik Shakked, Vice Chair
Lica Hartman
Christine Sublett

Members Absent

Dennis Chiu

Agenda Item	Comments/Discussion	Approvals/Action
1. CALL TO ORDER/ ROLL CALL	The open session meeting of the Corporate Compliance/Privacy and Internal Audit Committee of El Camino Hospital (the “Committee”) was called to order at 5:00pm by Chair Zoglin. A silent roll call was taken. Committee Member Chiu was absent. All other Committee members were present.	
2. POTENTIAL CONFLICT OF INTEREST DISCLOSURES	Chair Zoglin asked if any Committee members may have a conflict of interest with any of the items on the agenda. No conflicts were noted.	
3. PUBLIC COMMUNICATION	None.	
4. CONSENT CALENDAR	<p>Chair Zoglin asked if any member of the Committee or the public wished to remove an item from the consent calendar.</p> <p>Ms. Anolik Shakked requested that Agenda Item 4b: FY18 Meeting dates be removed. Ms. Anolik Shakked and Ms. Sublett explained that they are both not available on October 5th, but are available on September 28th. Ms. Wigglesworth noted that the auditors can only attend remotely on September 28th. Chair Zoglin requested that the auditors attend via videoconference.</p> <p>Motion: To approve the consent calendar: Meeting Minutes of the Open Session of the Corporate Compliance/Privacy and Internal Audit Committee (January 17, 2017); FY18 Meeting Dates.</p> <p>Movant: Anolik Shakked Second: Hartman Ayes: Anolik Shakked, Hartman, Sublett, Zoglin Noes: None Abstentions: None Absent: Chiu Recused: None</p>	<i>Consent Calendar approved</i>
5. REPORT ON BOARD ACTIONS	Chair Zoglin noted that the CEO search process is progressing. He also highlighted the strategic planning process with Manatt and conversation around mission, vision, and values. Donald Sibery, Interim CEO, noted that there is a special meeting of the Board on June 28 th for approval of the strategic plan. Chair Zoglin explained that the details of the priorities cannot be shared just yet. Chair Zoglin also noted that Neal Cohen, MD, will not returning as Hospital Board Chair and there are recruitment efforts from the District Board to fill his seat on the Board.	

6. FY18 PROPOSED COMMITTEEE GOALS

Diane Wigglesworth, Sr. Director, Corporate Compliance, explained that the proposed goals she drafted for FY18 revolve around three main categories:

1. **IT:** specifically Security Awareness Training, looking for Committee feedback on organization’s plan; this would be in addition to other IT reporting the Committee will receive.
2. **Compliance:** reorienting the organization on rules and policies regarding government investigations; this goal would cover education for the Board and the organization as a whole.
3. **Enterprise Risk:** an evolving process, including implementing structure, tying to strategy and overall risks; this goal would revolve around the Board’s engagement in Enterprise Risk and providing direction regarding risk tolerance levels.

In response to Ms. Anolik Shakked’s question, Mick Zdeblick, COO, clarified the timing on the Enterprise Risk goal, noting that the strategic process concludes in June, but an earlier timeframe would be feasible. He suggested proposing a framework in Q1 and implementation in Q2. Chair Zoglin suggested integrating the ERM discussion with the strategy discussion as appropriate, and picking one or two concrete risks to facilitate an explicit conversation rather than only the abstract “risk appetite.”

In response to Ms. Hartman’s question, Mr. Zdeblick explained that there is not a defined Enterprise Risk implementation plan yet. Ms. Hartman recommended that any Board educational session should explicitly define terms and methodology and use real scenarios as examples.

The Committee refined the goal to include an ERM roadmap (which includes a recommended framework) to be presented in Q1 and 1-2 concrete ERM discussions later in the year.

Ms. Anolik Shakked suggested adding a fourth goal to enable oversight of HIPAA Audit Readiness. The Committee members expressed their desire to see: 1) the same level of detail that has been provided for security to be provided for privacy matters as well and 2) validation (in whatever form staff deems appropriate) that ECH is HIPAA compliant (addressing gaps that assessments have identified). Ms. Wigglesworth suggested “provide validation of HIPAA Readiness to the Committee for review.” The Committee asked staff to determine what timeline would be appropriate for this goal. Ms. Wigglesworth noted that she would circulate an updated copy to the Compliance Committee ahead of the Governance Committee’s goal review in June.

Motion: To approve the Compliance Committee’s set of four proposed FY18 goals, with the edits as mentioned above to be forwarded to the Governance Committee for review.

Movant: Sublett

Second: Anolik Shakked

Ayes: Anolik Shakked, Hartman, Sublett, Zoglin

Noes: None

Abstentions: None

Absent: Chiu

Recused: None

Proposed FY18 Committee Goals recommended to the Governance Committee for review and approval

<p>7. PROPOSED FY17 FINANCIAL AUDIT PLAN</p>	<p>Ms. Wigglesworth distributed supplemental information from Moss Adams regarding factors that determine audit emphasis areas including: 1) risk assessment procedure (assigning a risk rating based on complexity of transaction and management judgments, e.g., long-term debt/bond refinancing) and 2) significant changes in operations for the organization (e.g., Epic implementation).</p> <p>The Moss Adams memo also noted that there is no set rotation of emphasis areas, but the areas identified in the risk assessment remain risks annually. New additions for 2017 include GASB No. 75 and new accounting for FASB. Moss Adams asked the Committee for their feedback on focus areas so long as they are within the scope of historical financial statement audits.</p> <p>The Committee discussed having more audit items on a rotational basis along with standard items and asked that formalized feedback/recommendations for the auditors be paced for the Committee’s May meeting.</p>	<p><i>Proposed FY17 audit plan paced for May 18, 2017 meeting</i></p>
<p>8. KPIs SCORECARD, AND TRENDS</p>	<p>Ms. Wigglesworth reviewed the KPI trends and noted there was an increase in hotline calls from patients noticing errors, due to increased access to and usage of MyChart. In response to a new issue raised, the IT team implemented a new process to migrate changes in Epic and other ambulatory systems over to MyChart. The Hospital also identified registration issues, where staff had not selected the correct individual as patients presented; Ms. Wigglesworth explained that there are two different processes to correct the error if the issue is discovered before or after the patient has been discharged.</p> <p>The Committee and staff discussed the migration issue between Epic and MyChart. Ms. Wigglesworth reported that there is a dedicated resource reviewing historical issues and verifying whether or not MyChart was impacted. Ms. Anolik Shakked suggested identifying and reviewing other corrections in Epic that may not have migrated over to MyChart.</p>	
<p>9. ADJOURN TO CLOSED SESSION</p>	<p>Motion: To adjourn to closed session at 5:36 pm pursuant to <i>Gov’t Code Section 54957.2</i> for approval of Meeting Minutes of the Closed Session of the Corporate Compliance/Privacy and Internal Audit Committee (January 17, 2017); pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Compliance Activity Log, Privacy Activity Log, Internal Audit Follow Up, Internal Audit Work Plan, FY17 Pacing Plan; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Report on Internal Audit Activity; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Legal Requirements for Board Compliance Education; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Board Compliance Education; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Summary of Physician Financial Arrangements; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Discussion on ERM Reporting; pursuant to <i>Gov’t Code Section 54956(d)(2)</i> – conference with legal counsel – pending or threatened litigation: Discussion on IT Security Plan; pursuant to <i>Gov’t Code Section 54957</i> for discussion and report on personnel matters:</p>	<p><i>Adjourned to closed session at 5:36pm.</i></p>

	<p>Executive Session.</p> <p>Movant: Anolik Shakked Second: Sublett Ayes: Anolik Shakked, Chiu, Hartman, Sublett, Zoglin Noes: None Abstentions: None Absent: None Recused: None</p>	
<p>10. AGENDA ITEM 20: RECONVENE OPEN SESSION/ REPORT OUT</p>	<p>Open session was reconvened at 7:14 pm. Agenda Items 9-19 were covered in closed session.</p> <p>During the closed session, the Committee approved the Closed Session Minutes of the Corporate Compliance/Privacy and Internal Audit Committee Meeting of January 17, 2017 and the Physician Financial Arrangements Summary by a vote of all members present (Anolik Shakked, Hartman, Sublett, Zoglin). Committee Member Chiu was absent.</p>	
<p>11. AGENDA ITEM 21: ADJOURNMENT</p>	<p>Motion: To adjourn at 7:16 pm.</p> <p>Movant: Anolik Shakked Second: Sublett Ayes: Anolik Shakked, Chiu, Hartman, Sublett, Zoglin Noes: None Abstentions: None Absent: None Recused: None</p>	<p><i>Meeting adjourned at 7:16pm.</i></p>

Attest as to the approval of the foregoing minutes by the Corporate Compliance/Privacy and Internal Audit Committee of El Camino Hospital:

John Zoglin
Chair, Corporate Compliance/
Privacy and Internal Audit Committee

Corporate Compliance/Privacy and Audit Committee Goals FY 2017

Purpose

The purpose of the Corporate Compliance/Privacy and Audit Committee (“Compliance and Audit Committee”) is to advise and assist the El Camino Hospital (ECH) Hospital Board of Directors (“Board”) in its exercise of oversight by monitoring the compliance policies, controls and processes of the organization and the engagement, independence and performance of the internal auditor and external auditor. The Compliance and Audit Committee assists the Board in oversight of any regulatory audit and in assuring the organizational integrity of ECH in a manner consistent with its mission and purpose.

Staff: Diane Wigglesworth, Senior Director, Corporate Compliance

The Senior Director, Corporate Compliance shall serve as the primary staff support to the Committee and is responsible for drafting the Committee meeting agenda for the Committee Chairs consideration. Additional members of the executive team or outside consultants may participate in the Committee meetings upon the recommendation of the Senior Director, Corporate Compliance and Internal Audit and at the discretion of the Committee Chair.

Goals	Timeline by Fiscal Year <small>(Timeframe applies to when the Board approves the recommended action from the Committee, if applicable.)</small>	Metrics of Success Achieved
<ul style="list-style-type: none"> ▪ Review and evaluate Hospitals Information Security Risk Management Plan 	<ul style="list-style-type: none"> ▪ Preliminary report in Q2 FY 2017 and Final report Q3 FY 2017 	<ul style="list-style-type: none"> ▪ Committee reviews and approves plan. Plan presented at 3/16/17 and 5/18/17 meetings.
<ul style="list-style-type: none"> ▪ Review and evaluate risk assessment of Patient Centered Medical Home (PCMH) Compliance and any corrective action plans 	<ul style="list-style-type: none"> ▪ Q3 FY 2017 	<ul style="list-style-type: none"> ▪ Committee reviews and approves plan. – Results of assessment and corrective actions presented at 1/19/17 meeting.
<ul style="list-style-type: none"> ▪ Review plan and evaluate ERM activities, performance and execution of program 	<ul style="list-style-type: none"> ▪ Q4 FY 2017 	<ul style="list-style-type: none"> ▪ Committee reviews and approves plan. ERM program updated presented at 3/16/17 and 5/18/17 meeting.

Submitted by:

John Zoglin, Chair, Corporate Compliance/Privacy and Audit Committee

Diane Wigglesworth, Executive Sponsor, Corporate Compliance/Privacy and Audit Committee

ECH BOARD COMMITTEE MEETING AGENDA ITEM COVER SHEET

Item:	Report on Board Actions Corporate Compliance/Privacy and Internal Audit Committee May 18, 2017
Responsible party:	Cindy Murphy, Board Liaison
Action requested:	For Information
Background:	In FY16, staff added this item to each Board Committee’s agenda to keep Committee members informed about Board actions via a verbal report by the Committee Chair. This written report is intended to supplement the Chair’s verbal report.
Other Board Advisory Committees that reviewed the issue and recommendation, if any:	None.
Summary and session objectives:	To inform the Committee about recent Board actions.
Suggested discussion questions:	None.
Proposed Committee motion, if any:	None. This is an informational item.
LIST OF ATTACHMENTS:	<ol style="list-style-type: none"> 1. Report on ECH April and May 2017 Board Actions

April and May 2017 ECH Board Actions*

1. April 12, 2017
 - a. Approved FY17 Period 8 Financials
 - b. Approved Primary Care Physician Replacement for Silicon Valley Primary Care Clinic
 - c. Approved Revisions to the Board Director Compensation Policy – Approved Annual Board Chair Stipend of \$12,000, payable quarterly and \$100 stipend for Committee Chair (Directors only) participation in agenda planning meeting.
 - d. Appointment of Executive Compensation Committee Member Pat Wadors
 - e. Approved Primary Care Physician Replacement for Silicon Valley Primary Care Clinic
 - f. Approved Finance Committee Recommendations:
 - i. SVPMG Physician Recruitment – Medical Oncologist
 - ii. General Surgery ED Call Panel
 - iii. Medical Directorship renewal – Quality and Physician Services
 - iv. Capital Funding Request – Women’s Hospital Expansion Incremental Funding
 - v. Capital Funding Request – Los Gatos Facility Improvement Project
2. May 10, 2017
 - a. Biennial Board Officer Election (for a two year term, effective July 1, 2017):
 - i. Hospital Board Chair – Lanhee Chen
 - ii. Hospital Board Vice Chair – John Zoglin
 - iii. Hospital Board Secretary/Treasurer – Julia Miller
 - b. Approved Revised Board Director Compensation Policy
 - c. Approved El Camino Hospital Auxiliary Slate of Officers

*This list is not meant to be exhaustive, but includes agenda items the Board voted on that are most likely to be of interest to or pertinent to the work of El Camino Hospital’s Board Advisory Committees.

ECH BOARD COMMITTEE MEETING AGENDA ITEM COVER SHEET

Item:	Approval of Policies Corporate Compliance/Privacy and Internal Audit Committee May 18, 2017
Responsible party:	Diane Wigglesworth, Sr. Director, Corporate Compliance
Action requested:	For Possible Motion
Background:	As required by Title 22 and The Joint Commission, the Hospital’s governing body must review and approve all organizational policies, plans, and scope of services at least every three years if there are no changes, and, if a policy is new or revised, it must be approved by the Board before the Hospital can adopt it. Policies are being brought to the appropriate Board Advisory Committee for review and recommendation before being placed on the Hospital Board consent calendar for approval. All policies have been internally reviewed and have received appropriate approvals before being presented to a Board Committee.
Other Board Advisory Committees that reviewed the issue and recommendation, if any:	None.
Summary and session objectives:	Review policies and recommend for Board approval.
Suggested discussion questions:	None.
Proposed Committee motion, if any:	To recommend that the Hospital Board approve the policies.
LIST OF ATTACHMENTS:	<ol style="list-style-type: none"> 1. Summary of Policy Changes <i>Policies</i> 2. Information Security: 1.04 Network Access Control 3. Information Security: 1.02 Authorized Access to Information Systems 4. Information Security: 0.01 Information Security Management Program 5. Information Security: 1.01 Business Requirement for Access Control 6. Information Security: 1.03 User Responsibilities 7. Corporate Compliance: 51.00 Physician Financial Arrangements – Review and Approval

SUMMARY OF POLICIES/PROTOCOLS FOR REVIEW AND APPROVAL

NEW POLICIES				
Policy Number	Policy Name	Department	Revised Date	Summary of Policy Changes
	1.04 Network Access Control	Information Security		Created new IT policies to meet regulatory and security requirements which will replace obsolete IT policies
	1.02 Authorized Access to Information Systems	Information Security		Created new IT policies to meet regulatory and security requirements which will replace obsolete IT policies
	0.01 Information Security Management Program	Information Security		Created new IT policies to meet regulatory and security requirements which will replace obsolete IT policies
	1.01 Business Requirement for Access Control	Information Security		Created new IT policies to meet regulatory and security requirements which will replace obsolete IT policies
	1.03 User Responsibilities	Information Security		Created new IT policies to meet regulatory and security requirements which will replace obsolete IT policies
POLICIES WITH MAJOR REVISIONS				
Policy Number	Policy Name	Department	Review or Revised Date	Summary of Policy Changes
	Physician Financial Arrangements	Administration	May 2017	Clarification of CEO authority for SV Primary Medical Group (SVPMG) PSA for individual employed physicians renewals or amendments.
POLICIES WITH MINOR REVISIONS				
Policy Number	Policy Name	Department	Review or Revised Date	Summary of Policy Changes
POLICIES WITH NO REVISIONS - REVIEWED				
Policy Number	Policy Name	Department	Review or Revised Date	Summary of Policy Changes
POLICIES TO ARCHIVE				
Policy Number	Policy Name	Department	DATE ARCHIVE	Summary of Policy Changes

TITLE: Information Security - 1.04 Network Access Control
CATEGORY: 1.0 Access Control
LAST APPROVAL:

TYPE: Policy Protocol Scope of Service/ADT
 Procedure Standardized Process/Procedure
SUB-CATEGORY: Information Security
OFFICE OF ORIGIN: InfoSec (ECH Solutions Group)
ORIGINAL DATE:

I. COVERAGE:

This policy applies to all workforce members, business associates and agents that access or uses El Camino Hospital information systems, IT assets, or medical devices. The workforce members may be defined as follows:

1. El Camino Hospital Employees, Physicians, Partners
2. Independent Contractors, Contract Services Personnel, Registry/Temporary Agency Personnel
3. Students, Interns, Instructors, Volunteers

II. PURPOSE:

To prevent unauthorized access to networked services.

III. POLICY STATEMENT:

It is the policy of El Camino Hospital that network equipment shall be physically protected from unauthorized access using network security technologies that provide capabilities for:

1. Authentication and Authorization mechanisms
2. Secure Communications and Transmissions
3. Remote Diagnostics and Monitoring
4. Virtual Private Network
5. Segmentation

IV. DEFINITIONS (if applicable):

IT - Information Technology
ISD - Information Services Division
ISO - Information Security Office

V. REFERENCES:

This policy enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Joint Commission Information Management, Payment Card

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.

TITLE: Information Security - 1.04 Network Access Control

CATEGORY: 1.0 Access Control

LAST APPROVAL:

Industry (PCI), National Institute of Standards and Technology (NIST) plus other applicable state laws and standards.

VI. PROCEDURE:

The procedures that implement this policy are documented under the following titles:

A. 1.i Policy on the Use of Network Services

1.j User Authentication for External Connections

1.k Equipment Identification in Network

1.l Remote Diagnostic and Configuration Port Protection

1.m Segregation in Networks

1.n Network Connection Control

1.o Network Routing Control

B. Progressive Sanctions

1. A progressive sanction process consistent with the “**HR-Discipline and Discharge**” policy may be enforced by the Information Security Office (**ISO**) for IT Security policy and procedure violations that are caused by negligence or unawareness.
2. Workforce members may be requested to attend Security Awareness training specifically designed to mitigate misunderstandings regarding individual responsibilities to comply with policies and procedures.

C. RESPONSIBILITIES:

1. Network Engineering with support from the ISO shall conduct reviews to ensure network equipment is protected from unauthorized access, including identifying and disabling non-secure functions, ports, protocols, software and services.
2. The ISO shall provide leadership and guidance to all business functions in regards to identifying and mitigating security and compliance concerns that impacts access to information and information assets.
3. The ISO shall facilitate security focus groups; implement toolsets, standards and technical safeguards that incorporate stakeholder business objectives with risk acceptance approved by the IT Security Program Executive Steering Committee.

TITLE: Information Security - 1.04 Network Access Control
CATEGORY: 1.0 Access Control
LAST APPROVAL:

VII. APPROVAL:

APPROVING COMMITTEES AND AUTHORIZING BODY	APPROVAL DATES
InfoSec – CISO	2/14/2017
Information Services Division - CIO	3/21/2017
ePolicy Committee:	5/5/2017
Medical Executive Committee:	
Board of Directors:	
Historical Approvals:	

VIII. ATTACHMENTS (if applicable): N/A

TITLE: Information Security - 1.02 Authorized Access to Information Systems
CATEGORY: 1.0 Access Control
LAST APPROVAL:

TYPE: Policy Protocol Scope of Service/ADT
 Procedure Standardized Process/Procedure

SUB-CATEGORY: Information Security Office
OFFICE OF ORIGIN: Information Services Division
ORIGINAL DATE:

I. COVERAGE:
 This policy applies to all workforce members, business associates and agents that access or uses El Camino Hospital information systems, IT assets, or medical devices. The workforce members maybe defined as follows:

1. El Camino Hospital Employees, Physicians, Partners
2. Independent Contractors, Contract Services Personnel, Registry/Temporary Agency Personnel
3. Students, Interns, Instructors, Volunteers

II. PURPOSE:
 To ensure authorized user accounts are registered, tracked and periodically validated to prevent unauthorized access to information systems.

III. POLICY STATEMENT:
 It is the policy of El Camino Hospital that a formal user registration procedure be used to track the authorized access to ECH information systems, IT assets, or medical devices. A documented user registration and deregistration process for granting, suspending, and revoking access shall be maintained and the practice of performing annual recertification of user access shall be implemented.

IV. DEFINITIONS (if applicable):
ePHI – electronic Protected Health Information
PII - Personally identifiable information
FIN –financial data
SD – sensitive data for the business enterprise, includes confidential and intellectual property

V. REFERENCES:
 This policy enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Joint Commission Information Management, Payment Card

***NOTE:** Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.*

TITLE:	Information Security - 1.02 Authorized Access to Information Systems
CATEGORY:	1.0 Access Control
LAST APPROVAL:	

Industry (PCI), National Institute of Standards and Technology (NIST) plus other applicable state laws and standards.

VI. PROCEDURE:

The procedures that implement this policy are documented under the following titles:

A. 1.b User Registration

1.c Privilege Management

1.d User Password Management

1.e Review of User Access Rights

B. Progressive Sanction

1. A progressive sanction process consistent with the “**HR-Discipline and Discharge**” policy may be enforced by the Information Security Office (ISO) for IT Security policy and procedure violations that are caused by negligence or unawareness.
2. Workforce members may be requested to attend Security Awareness training specifically designed to mitigate misunderstandings regarding individual responsibilities to comply with policies and procedures.

C. RESPONSIBILITIES:

1. System Administrators shall review accounts quarterly and disable any account that is inactive beyond 60 days or that cannot be associated with a valid business owner or service account. Leaders shall recertify user access to information systems, IT assets, and medical devices that contain ePHI, PII, FIN, or SD and provide documented evidence to the ISO for review and record retention.
2. The ISO shall provide leadership and guidance to all business functions in regards to identifying and mitigating security and compliance concerns that impacts access to information and information assets.
3. The ISO shall facilitate security focus groups; implement toolsets, standards and technical safeguards that incorporate stakeholder business objectives with risk acceptance approved by the IT Security Program Executive Steering Committee.

TITLE: Information Security - 1.02 Authorized Access to Information Systems
CATEGORY: 1.0 Access Control
LAST APPROVAL:

VII. APPROVAL:

APPROVING COMMITTEES AND AUTHORIZING BODY	APPROVAL DATES
InfoSec – CISO	2/14/2017
Information Services Division - CIO	3/21/2017
ePolicy Committee:	5/5/2017
Medical Executive Committee:	
Board of Directors:	
Historical Approvals:	

VIII. ATTACHMENTS (if applicable): N/A

TITLE: Information Security – 0.01 Information Security Management Program
CATEGORY: Information Security Management Program
LAST APPROVAL:

TYPE: Policy Protocol Scope of Service/ADT
 Procedure Standardized Process/Procedure
SUB-CATEGORY: Information Security Office
OFFICE OF ORIGIN: Information Services Division
ORIGINAL DATE:

I. COVERAGE:
 This policy applies to all workforce members, business associates and agents that access or uses El Camino Hospital information systems, IT assets, or medical devices. The workforce members maybe defined as follows:

1. El Camino Hospital Employees, Physicians, Partners
2. Independent Contractors, Contract Services Personnel, Registry/Temporary Agency Personnel
3. Students, Interns, Instructors, Volunteers

II. PURPOSE:
 To implement and manage an Information Security Management Program.

III. POLICY STATEMENT:
 It is the policy of El Camino Hospital that Technical Services, Clinical Engineering and the Information Security Office (ISO) shall work collaboratively to develop, implement and maintain an Information Security Management Program that is based on security and compliance requirements that effectively supports the enterprise business. An Information Security Management System shall be established to be the central repository of artifacts used for monitoring, maintaining and improving the enterprise security posture.

The ISMS shall contain reasonable documentation to demonstrate evidence that administrative, technical, and physical safeguards exist for the maintenance of an effective Information Security Management Program.

IV. DEFINITIONS (if applicable):
ISD – Information Services Division
ISO – Information Security Office
ISMS - is a set of policies and procedures that addresses workforce members’ behaviors in the management of El Camino Hospitals’ sensitive data and technologies. The overall goal

TITLE:	Information Security – 0.01 Information Security Management Program
CATEGORY:	Information Security Management Program
LAST APPROVAL:	

is to minimize unnecessary risk by pro-actively limiting the impact a security breach could have on business continuity.

V. REFERENCES:

This policy enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Joint Commission Information Management requirements, Payment Card Industry (PCI), National Institute of Standards and Technology (NIST) plus other applicable state laws and standards.

VI. PROCEDURE:

The procedure that implements this policy is documented under the following title:

A. a Information Security Management Program

B. Progressive Sanction

1. A progressive sanction process consistent with the “**HR-Discipline and Discharge**” policy may be enforced by the Information Security Office (ISO) for IT Security policy and procedure violations that are caused by negligence or unawareness.
2. Workforce members may be requested to attend Security Awareness training specifically designed to mitigate misunderstandings regarding individual responsibilities to comply with policies and procedures.

C. RESPONSIBILITIES:

1. The ISO shall provide leadership and guidance to all business functions in regards to identifying and mitigating security and compliance concerns that impacts access to information systems, IT assets and medical devices.
2. The ISO shall facilitate security focus groups; implement toolsets, standards and technical safeguards that incorporate stakeholder business objectives with risk acceptance approved by the IT Security Program Executive Steering Committee.

TITLE: Information Security – 0.01 Information Security Management Program
CATEGORY: Information Security Management Program
LAST APPROVAL:

VII. APPROVAL:

APPROVING COMMITTEES AND AUTHORIZING BODY	APPROVAL DATES
InfoSec – CISO	2/14/2017
Information Services Division - CIO	3/21/2017
ePolicy Committee:	5/5/2017
Medical Executive Committee:	
Board of Directors:	
Historical Approvals:	

VIII. ATTACHMENTS (if applicable): N/A

TITLE: Information Security - 1.01 Business Requirement for Access Control

CATEGORY: 1.0 Access Control

LAST APPROVAL:

TYPE:

- Policy Protocol Scope of Service/ADT
 Procedure Standardized Process/Procedure

SUB-CATEGORY: Information Security Office

OFFICE OF ORIGIN: Information Services Division

ORIGINAL DATE:

I. COVERAGE:

This policy applies to all workforce members, business associates and agents that access or uses El Camino Hospital information systems, IT assets, or medical devices. The workforce members maybe defined as follows:

1. El Camino Hospital Employees, Physicians, Partners
2. Independent Contractors, Contract Services Personnel, Registry/Temporary Agency Personnel
3. Students, Interns, Instructors, Volunteers

II. PURPOSE:

To control access to information, information assets, and business processes based on business and security requirements.

III. POLICY STATEMENT:

It is the policy of El Camino Hospital that our business requirements and access control rules shall be communicated to users and service providers prior to granting them access to ECH information systems, IT assets, or medical devices.

IV. DEFINITIONS (if applicable):

IT - Information Technology
ISD - Information Services Division
ISO - Information Security Office

V. REFERENCES:

This policy enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Joint Commission Information Management, Payment Card Industry (PCI), National Institute of Standards and Technology (NIST) plus other applicable state laws and standards.

TITLE:	Information Security - 1.01 Business Requirement for Access Control
CATEGORY:	1.0 Access Control
LAST APPROVAL:	

VI. PROCEDURE:

The procedure that implements this policy is documented under the following title:

A. 1.a Access Control Policy

B. Progressive Sanction

1. A progressive sanction process consistent with the “**HR-Discipline and Discharge**” policy may be enforced by the Information Security Office (ISO) for IT Security policy and procedure violations that are caused by negligence or unawareness.
2. Workforce members may be requested to attend Security Awareness training specifically designed to mitigate misunderstandings regarding individual responsibilities to comply with policies and procedures.

C. RESPONSIBILITIES:

1. The Information Services Division and information systems, IT assets and medical devices' owners shall ensure business requirements and access control rules are communicated to ensure users and service providers adhere to our access control policy.
2. The ISO shall provide leadership and guidance to all business functions in regards to identifying and mitigating security and compliance concerns that impacts access to information and information assets.
3. The ISO shall facilitate security focus groups; implement toolsets, standards and technical safeguards that incorporate stakeholder business objectives with risk acceptance approved by the IT Security Program Executive Steering Committee.

VII. APPROVAL:

APPROVING COMMITTEES AND AUTHORIZING BODY	APPROVAL DATES
InfoSec – CISO	2/14/2017
Information Services Division - CIO	3/21/2017
ePolicy Committee:	5/5/2017
Medical Executive Committee:	
Board of Directors:	
Historical Approvals:	

VIII. ATTACHMENTS (if applicable): N/A

TITLE:	Information Security - 1.03 User Responsibilities
CATEGORY:	1.0 Access Control
LAST APPROVAL:	

TYPE:	<input checked="" type="checkbox"/> Policy <input type="checkbox"/> Protocol <input type="checkbox"/> Scope of Service/ADT <input type="checkbox"/> Procedure <input type="checkbox"/> Standardized Process/Procedure
SUB-CATEGORY:	Information Security
OFFICE OF ORIGIN:	InfoSec (ECH Solutions Group)
ORIGINAL DATE:	

- I. **COVERAGE:**
 This policy applies to all workforce members, business associates and agents that access or uses El Camino Hospital information systems, IT assets, or medical devices. The workforce members maybe defined as follows:
 1. El Camino Hospital Employees, Physicians, Partners
 2. Independent Contractors, Contract Services Personnel, Registry/Temporary Agency Personnel
 3. Students, Interns, Instructors, Volunteers

- II. **PURPOSE:**
 To prevent unauthorized user access and compromise or theft of information and information assets.

- III. **POLICY STATEMENT:**
 It is the policy of El Camino Hospital that verbal communication, signs, emails, newsletters, videos, warning banners, and websites shall be the primary tools used to inform users of their responsibilities to adhere to good security practices. The topics shall focus on password protection, equipment usage, media disposition, and clear desk/screen practices for safeguarding sensitive data from unauthorized access.

- IV. **DEFINITIONS (if applicable):**
 IT - Information Technology
 ISD - Information Services Division
 ISO - Information Security Office

- V. **REFERENCES:**
 This policy enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, Joint Commission Information Management, Payment Card Industry (PCI), National Institute of Standards and Technology (NIST) plus other applicable state laws and standards.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.

TITLE: Information Security - 1.03 User Responsibilities

CATEGORY: 1.0 Access Control

LAST APPROVAL:

VI. PROCEDURE:

The procedures that implement this policy are documented under the following titles:

A. 1.f Password Use

1.g Unattended User Equipment

1.h Clear Desk and Clear Screen Policy

B. Progressive Sanctions

1. A progressive sanction process consistent with the “**HR-Discipline and Discharge**” policy may be enforced by the Information Security Office (**ISO**) for IT Security policy and procedure violations that are caused by negligence or unawareness.
2. Workforce members may be requested to attend Security Awareness training specifically designed to mitigate misunderstandings regarding individual responsibilities to comply with policies and procedures.

C. RESPONSIBILITIES:

1. ISD with support from the ISO shall ensure annual education will be provided to all workforce members covering these topics. Leaders shall ensure all workforce members within their areas of responsibilities are properly informed and remain compliant with the password protection, equipment usage, media disposition and clear/desk screen safeguarding practices.
2. The ISO shall provide leadership and guidance to all business functions in regards to identifying and mitigating security and compliance concerns that impacts access to information and information assets.
3. The ISO shall facilitate security focus groups; implement toolsets, standards and technical safeguards that incorporate stakeholder business objectives with risk acceptance approved by the IT Security Program Executive Steering Committee.

TITLE: Information Security - 1.03 User Responsibilities
CATEGORY: 1.0 Access Control
LAST APPROVAL:

VII. APPROVAL:

APPROVING COMMITTEES AND AUTHORIZING BODY	APPROVAL DATES
InfoSec – CISO	2/14/2017
Information Services Division - CIO	3/21/2017
ePolicy Committee:	5/5/2017
Medical Executive Committee:	
Board of Directors:	
Historical Approvals:	

VIII. ATTACHMENTS (if applicable): N/A



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

SUB-CATEGORY: Administrative Policies and Procedures
ORIGINAL DATE: 6/08

COVERAGE:

All El Camino Hospital staff, Contract Personnel, Physicians, Healthcare Providers, and the Governing Board

PURPOSE:

The purpose of this policy is to comply with the Stark law, Anti-Kickback, HIPAA and all other Federal and State Laws.

STATEMENT:

This policy implements the overall compliance goals of the Hospital with respect to Physician financial arrangements.

This policy establishes administrative principles and guidelines, Board delegation of authority and oversight, and review processes and approvals that must be followed before the Hospital enters into a direct or indirect financial arrangement with an individual physician, a physician group, other organizations representing a physician, or a member of immediate family of a physician ("Physician"). Physician financial arrangements that involve any transfer of value, including monetary compensation, are subject to this and the following policies: 1) Signature Authority policy 17.00, 2) Reimbursement of Business Expenses policy 5.00, and 3) Physician Recruitment policy 42.00.

All financial arrangements of any kind involving Physician, including but not limited to, medical director, consulting, on-call arrangements, professional service agreements, education and training, conference reimbursement or real estate leases, will comply with the Stark law, Anti-Kickback, HIPAA and all other Federal and State Laws.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

All Physician financial arrangements are prohibited except those Physician financial arrangements that are approved and documented as provided in this Policy.

Physician financial arrangements may be entered into only where they are needed and serve the strategic goals (including quality and value) of the Hospital. Each Physician financial arrangement must meet or exceed the complex and stringent legal requirements that regulate Physician financial relationships with the Hospital. All Physician financial arrangements between a physician and the Hospital must be in writing and meet fair market value, commercial reasonableness and the following requirements as applicable.

PROCEDURE:

A. **Administrative Standards:**

When creating or renewing a Physician financial arrangement, the following principles must be followed. This Policy applies to any Physician financial arrangement including, but not limit to: Medical Directorships, ED Call Panels, Professional Services, Panel Professional Services, Consulting, Lease, Education and Training, Conference Payment, and Physician Recruitment.

1. **All Physician Financial Arrangements:**

- a) Each Physician financial arrangement (except Physician Lease Contracts) must provide a service that is needed for at least one of the following reasons: 1) it is required by applicable law, 2) required administrative or clinical oversight can only be provided by a qualified physician, 3) the administrative services to be provided support an articulated strategic goal of the Hospital, such as patient safety, and 4) the arrangement must solve, prevent or mitigate an identified operational problem for the Hospital.
- b) The terms of the Physician financial arrangement must be fair market value and commercially reasonable and must not take into account the volume or value of any referrals or other business generated between the parties. All of the terms of the Physician financial arrangement must be in a written contract that details the work or activities to be performed

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

and all compensation of any kind or the lease terms (“Physician Contracts”). The services contracted for may not exceed those that are reasonable and necessary for the legitimate business purposes of the Physician financial arrangement. If there is more than one Physician Contract with a Physician, the Physician Contracts must cross-reference one another (or be identified on a list of Physician Contracts) and be reviewed for potential overlapping commitments prior to negotiating additional agreements.

The process for determining Physician compensation for each Physician financial arrangement must be set forth in the Physician Contract file and identified in sufficient detail so that it can be objectively verified as meeting fair market value standards. Any compensation paid to or remuneration received by a Physician shall not vary based on the volume or value of services referred or business otherwise generated by the Physician and must reflect fair market value. Compensation cannot exceed the seventy-fifth percentile of fair market value without prior Board approval. ~~Medical Director Agreements should use national market data and On-Call agreements~~ All Physician contracts should use local or regional market data, when available, to determine the seventy-fifth percentile of FMV.

In order to support reasonableness of compensation or remuneration, written fair market data must accompany the Physician Contract and show compensation paid by similar situated organizations and/or independent compensation surveys by nationally recognized independent firms.

- c) Compensation cannot be revised or modified during the first twelve (12) months of any Physician financial arrangement. If the compensation is revised thereafter, it must be evidenced by a written amendment to the Physician Contract, signed by both parties before the increase in compensation takes effect. For example, if the increase in compensation is to take effect on April 1, the amendment must be signed by both parties on or before April 1 and the original Physician Contract must have been effective on or before March 31 of the prior year. The compensation cannot be changed for twelve (12) months after the effective date of such amendment.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

- d) All Physician Contract renewals must be signed before the expiration of the term of the existing Physician Contract.
- e) Physician Contracts must be in writing and executed by the parties before commencement. Only the CEO of Hospital may execute a Physician Contract, except Physicians Contracts that are real estate or equipment leases with Physicians may be signed by the Chief Administrative Services Officer (“CASO”). Physicians cannot be compensated for work performed, nor may a lease commence, prior to execution by both parties.
- f) The Physician financial arrangement must not violate the Stark law, the anti-kickback statute (section 1128B(b) of the Act) or any Federal or State law or regulations.
- g) The Physician Contract will permit the Hospital to suspend performance under the Physician Contract if there is a compliance concern. Concerns about compliance should be directed to Compliance, Legal, or the office of the Chief Medical Officer (“CMO”). Performance under Physician Contracts deemed to not meet the administrative guidelines shall be suspended until the Physician Contract can be remedied.
- h) Physician Contracts must contain termination without cause provisions (except for real estate and equipment leases). Physician Contracts which grant an exclusive right to Hospital-based physicians to perform services may not exceed five years. If a Physician Contract is terminated, then the Hospital may not enter into a new financial arrangement with the same Physician covering the same arrangement on different terms within twelve (12) months of the effective date of the terminated Physician Contract.
- i) Physicians with potential conflicts of interest must complete a conflict of interest form (see Policy 4.00) that must be reviewed by the Compliance Officer prior to entering into a Physician Contract. The conflict must be addressed and referenced in the Physician Contract. A conflict may prevent entry into a Physician Contract.
- j) All Physician Contracts must be prepared using the appropriate Hospital contract template prepared by Legal ~~and Contracting~~ Services. All



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

Physician Contracts must be drafted by personnel designated by Legal ~~and Contracting~~ Services.

- k) Attached to the final version of a Physician Contract prior to execution by Hospital must be a completed “~~Contract Cover Sheet and Summary of Terms~~ **Physician Arrangement Review Checklist**” and a signed “**Certification of Necessity and Fair Market Value**” ~~Contract Certification~~” (Appendix A) (a Physician Lease Contract must also include a signed “**Contract Certification**” (Appendix B) and “**Lease Contract Review Checklist**” (Appendix ~~BC~~) to be reviewed and approved by Legal ~~and Contracting~~ Services and Compliance.
 - l) All executed Physician Contracts must be scanned into the Meditract system.
 - m) Payments may not be made to a Physician unless there is adherence with all of the requirements of this Policy.
 - n) Each Physician Contract shall comply with all applicable laws.
2. **Medical Director Contracts:** In addition to the criteria set forth above (D.1) for *All Physician Financial Arrangements*, the following must be met *prior* to creating, renewing or amending a Medical Directorship:
- a) A Medical Directorship may not be intended or used as a means to recruit a Physician to practice at the Hospital.
 - b) A Medical Directorship must fit within a rational management framework that optimizes coordination of the Medical Director’s knowledge and work efforts with Hospital needs and resources. To meet this requirement, the Medical Director must work with, and be accountable to, a supporting Hospital manager-partner who is a Hospital supervisor, manager or executive director who verifies the Medical Director’s work and efforts. The Hospital manager-partner shall participate in the negotiation of the Medical Director Contract, including setting duties and goals, and will be familiar with the details of the Medical Director Contract.
 - c) The number of hours assigned to the Medical Directorship must be appropriate considering the work required. An annual evaluation shall

Formatted: Highlight

Formatted: Highlight



POLICY/PROCEDURE TITLE: Corporate Compliance:51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

be conducted by the CMO and the Hospital manager-partner to evaluate whether all such services are needed in any new or renewal term, whether new services are needed and if the hours are still reasonable and necessary for the legitimate business purpose of the Medical Directorship arrangement. The proposed services may not duplicate work that is provided to the Hospital by other Physicians unless the total work under all arrangements are needed.

- d) Medical Director Contracts must require Physician completion and submission of Physician Time Study Reports (see Exhibit C) each month, and each such report must be approved by the Hospital manager-partner and the Compliance Department before any compensation is paid. There must be one or more internal review processes to verify that the Medical Director is performing the expected duties and tasks, of which the required time report is one example.
- e) All Medical Director Contracts providing for total compensation of \$30,000 or more shall include two (2) annual quality incentive goals that support the Hospital's strategic initiatives, one of which shall be related to an outcome quality metric and the other shall be related to a process metric or milestone for service to patients. For Medical Director Contracts greater than \$100,000 in compensation per year, 20% of the total compensation will be held at risk based on the completion of the quality incentive goals. For Medical Director Contracts between \$50,000 to \$99,999 per year, 10% of the total compensation will be held at risk based on the completion of the goals. For Medical Director Contracts between \$30,000 to \$49,999 per year, 5% of the total compensation will be held at risk based on the completion of the goals.
- f) If a Medical Director would oversee a function in a service line, then a development and selection committee (that includes at least one physician leader in the service line) will evaluate the candidates and recommend a final candidate with whom the Hospital should negotiate. An effective alignment of the Physician and the service line should be created.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

- g) If the Medical Directorship is intended to oversee a function outside of a defined service line, the CMO will evaluate and approve the Medical Director candidates for the proposed function.
- h) Each year, the Medical Executive Committee will review a summary report of all Medical Directorship arrangements and goals.
- i) Medical Director Contracts must include a Hospital-approved HIPAA Business Associate Agreement.

3. Physician Consulting Contracts:

In addition to the criteria set forth in the *All Physician Financial Arrangements* section (D.1) above, the following criteria must be met *before* creating or renewing a Physician Consulting Contract:

- a) Physician Consulting Contracts must require concise deliverables and due dates and require completion of a Physician Time Study Report (see Exhibit C). The deliverables and due dates must be set for the duration of the Physician Consulting Contract before the services begin and the Physician Consulting Contract is signed.
- b) The number of hours assigned to the Physician Consulting Contract must be appropriate in light of the work required.
- c) Physician Consulting Contracts must include a Hospital-approved HIPAA Business Associate Agreement.

4. Physician Lease Contracts:

In addition to the criteria set forth in the *All Physician Financial Arrangements* section above (D.1), the following criteria must be met *before* creating, amending, or renewing a Physician Lease Contract:

- a) Attached to the final version of a Physician Lease Contract, and prior to execution, must be a completed "Lease Contract Review Checklist" (Appendix ~~BC~~) and ~~applicable sections of Appendix A and~~ an executed "Contract Certification" (Appendix B).
- b) Tenant Improvements must be incorporated into the Physician Lease Contract as a Tenant expense.

POLICY/PROCEDURE TITLE: Corporate Compliance:51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

- c) Physician must not use the space and the Hospital must not make the space available for use prior to the execution of the Physician Lease Contract by both parties.
 - d) The Physician Lease Contract shall require that all property taxes are to be paid by the Tenant for Triple Net leases.
 - e) Physician Lease Contracts are executed by the CEO or the CASO.
5. **Physician Education, Training and Conference Payment Contracts:**
In addition to the criteria set forth in the *All Physician Financial Arrangements* section above (D.1) , the following criteria must be met *before* creating a new Education, Training and Conference Reimbursement Contracts and prior to attendance:
- a) Physician Education, Training and Conference Payment Contracts must be created and reimbursed in accordance with Hospital Policy Reimbursement of Business, Education and Travel Expenses (see Hospital Policy 5.00).
 - b) The Hospital’s need for this training to be provided to the Physician shall be documented as part of the approval process.
6. **Physician Recruitment Contracts:**
In addition to the criteria set forth in the *All Physician Financial Arrangements* section above (D.1), the following criteria must be met *before* creating a new Physician Recruitment Contract:
- a) Physician Recruitment Contracts must be created in accordance with the Physician Recruitment Policy Program, (see Hospital Policy 42.00) and must be presented to the Board for review before the recruitment proposal is developed.

B. Approval of Physician Contracts:

1. Attached to the final version of a Physician Contract *before* CEO execution must be a completed “Contract Cover Sheet and Summary of Terms” and “Certification of Necessity and Fair Market Value” ~~Physician Arrangement Review Checklist~~ and signed “Contract Certification” (Appendix A).
2. Attached to the final version of a Physician Lease Contract, *prior* to execution by the CEO or the CASO, must be a completed “Lease Contract Review Checklist” (Appendix BC) and ~~a completed “Physician Arrangement Review Checklist”~~ and signed “Contract Certification” (Appendix AB).

Formatted: Highlight



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

3. Corporate Compliance and the ~~General Counsel~~ Director of Legal & Contracting Services will verify the checklist, certification, and documentation accompanying all Physician Contracts (including FMV) prior to execution by the CEO or the CASO. Incomplete or missing checklist and certifications will be returned to the originator for completion.
4. All proposed Physician Contracts lacking the appropriate documentation will be returned to the originator for completion. No services may be performed under the Physician Contract or leases implemented until the Physician Contract is fully executed.
5. CEO Approval: The CEO will have authority to execute new, renewal and amended Physician Contracts (up to \$250,000.00 in total possible compensation annually), except as set forth in Section 6(b) below.

If a new arrangement is over \$250,000.00; or a renewal or amended agreement is over \$250,000; or the annual increase is greater than ten percent (10%), the Board must approve prior to CEO execution, except as set forth in Section 6(b) below. All recruitment proposals must be approved prior to the CEO executing.

6. Board Approval:
 - a. If a new arrangement is over \$250,000.00; or a renewal or amended agreement is over \$250,000; or the annual increase is greater than ten percent (10%), the Board must approve prior to CEO execution of the Physician Contract.
 - 1) All new Physician financial arrangements that exceed \$250,000 annually should be presented to the appropriate Board Committees for review and recommendation to the Board of Directors prior to being placed on the Board of Directors' agenda and prior to execution.
 - 2) A memo prepared by Hospital-Manager Partner that justifies the Hospital's needs shall be provided to the appropriate Board Committees and Board of Directors as part of the approval documents.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

2) b. Notwithstanding Section 6(a), the CEO may execute without Board approval a renewal or amended Professional Services Agreement with SV Primary Medical Group, P.C. ("SVPMG") so long as the total cash compensation to each individual physician employed by SVPMG does not exceed 75% percentile of fair market value or \$1,000,000 annually.

Formatted: Indent: Left: 0.5", No bullets or numbering

C. Board Oversight and Internal Review Process:

During the second and fourth quarter of each Hospital fiscal year, management and staff will prepare a summary report for all Physician financial arrangements describing: 1) the names of all such arrangements and associated physicians, 2) the organizational need that justifies each arrangement, 3) the total amounts paid to each physician and/or group for each Physician Contract annually (and in total for duration of contract term), 4) current and prior year annual financial comparison, 5) Education, Training or Conference Contracts that reimburse for travel expenses out of the state of California, and 6) any recommendations for changes to the Policy or any procedure.

For Medical Directorships, the summary report will also include: 1) the goals set forth for each Medical Directorship, 2) the contracted rate and hours, and 3) assessment of the performance of Medical Directors over the past year.

The CFO, COO & CMO will review the information and prepare recommendations if any regarding specific actions or changes that will be implemented.

The report will then be reviewed by the CEO and presented to the Compliance and Finance committees of the Board of Directors for review and submission to the Board of Directors no later than the end of the following quarter.

D. Exceptions:

There are no exceptions to this Policy unless approved by the Board of Directors in advance.

E. Review and/or Validate:

The CEO and the Corporate Compliance Officer shall be responsible for reviewing the policy and guidelines as conditions warrant but at a minimum at



POLICY/PROCEDURE TITLE: Corporate Compliance:51.00 Physician Financial Arrangements - Review and Approval
Last Approval Date: 05/14

least annually to assure consistency with Board expectations. The Compliance department will annually monitor organizations adherence to the policy and report to the Board.

F. Policy Enforcement

El Camino Hospital’s Compliance Officer is responsible for monitoring enforcement of this policy. Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPROVAL	APPROVAL DATES
Originating Committee or UPC Committee:	
Medical Committee (if applicable):	
ePolicy Committee: (Please don't remove this line)	
Pharmacy and Therapeutics (if applicable):	
Medical Executive Committee:	
Board of Directors:	

Historical Approvals:

New 6/08, 06/09; 8/12, 10/12, 11/13, 1/14, 5/14

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval

APPENDIX A
ECH Contract Cover Sheet and Summary of Terms

Physician/Physician Group Name Party to Agreement:

Type of Agreement: Medical Director Consulting Services Professional Services
 ED Call Hospital-Based Physician Services
 Other:

Agreement is: New Amendment Extension Renewal

Department/Program:

Campus:

Designated ECH Manager:

Effective Date:

Expiration Date:

Need for Agreement:

Reason Physician or Physician group was chosen for the position:

Number of Hours to be Worked:

Hourly/PerDiem Rate to Physician/Physician Group:

Does Agreement include two Quality Goals for Medical Directorships, if Total Annual Compensation is greater than \$30,000.00 annually:

Total Annual Amount:

Finance Committee Review and Board approval required under Policy 51.00:

No Yes (if yes, attach approval documentation)

Approvals

Compliance: _____ Date: _____

Legal: _____ Date: _____

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval

CERTIFICATION OF NECESSITY AND FAIR MARKET VALUE:

I certify that: (1) the services to be provided by Physician/Medical Group are reasonable and necessary because

____; and (2) the compensation proposed for this arrangement is fair market value because (check one):

___ MD Rater Data attached hereto, is at or below the 75th percentile, or

___ I have a FMV opinion, attached hereto, which demonstrates fair market value.

Signature: _____
Designated ECH Manager

APPENDIX B

Compliance Checklist

- Yes No 1. ~~Has the amount of compensation been determined based on the volume or value of any actual or anticipated referral by the physician or other business generated by the parties?~~
- Yes No 2. ~~Do aggregate services contracted or space or equipment leased exceed those that are reasonable and necessary for legitimate business purposes of the arrangement?~~
- Yes No 3. ~~Are any payments or other consideration made in consideration of, or to obtain, referrals?~~
- Yes No 4. ~~Do the services to be furnished involve counseling or promotion of any arrangement or other activity that violates any state or federal law?~~
- Yes No 5. ~~Has the Hospital paid the Physician including an immediate family member any amount of money within the last 12 months?~~
- Yes No 6. ~~Other than this Physician Contract, will the Hospital pay the Physician including an immediate family member any amount of money within the next 12 months?~~
- Yes No 7. ~~Were any loans or loan guarantees made by Hospital to the Physician?~~
- Yes No 8. ~~Will there be any non-monetary compensation to the Physician?~~
- Yes No 9. ~~Has this Physician Contract been executed, terminated or modified, or has it expired within the last 12 months?~~
- Yes No 10. ~~Is there another Physician arrangement at the Hospital with similar duties and responsibilities?~~
- Yes No 11. ~~Does the Physician Contract automatically renew?~~
- Yes No 12. ~~Were any of the approved contracts' standard terms modified? If yes, attach a copy marked to show changes~~
- Yes No 13. ~~Does the Physician currently have any other financial arrangement with the Hospital?~~
- Yes No 14. ~~If yes, are the other arrangements identified in the current Physician Contract, or on a master list?~~



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval

- Yes No 15. Has the Physician completed a conflict of interest disclosure form?
- Yes No 16. Are the services needed by the Hospital to carry out its tax exempt mission?
- Yes No 17. Has a fair market value (FMV) analysis been completed?
- Yes No 18. Is the analysis attached? Who completed the FMV analysis? _____
- Yes No 19. Do all of the services contracted for or lease price meet reasonable FMV?
- Yes No 20. Was the amount ECH was willing to pay determined before negotiations with the Physician?
- Yes No 21. Does the Physician Contract clearly detail the scope of work, all the services, duties and responsibilities and/or deliverables to be furnished by the Physician?
- Yes No 22. Are all the referenced documents (attachments or exhibits) complete and submitted with the final Physician Contract and certification?
- Yes No 23. If this is a Medical Director Contract, have "quality outcome goals" been included in the contract?
- Yes No 24. If this is a Medical Director Contract, has Medical Executive Committee approved? Date Approved by Medical Executive Committee: _____
- Yes No 25. Is the term of the arrangement for at least one year?
- Yes No 26. Is it possible to cancel/terminate the Physician Contract for failure to perform?
- Yes No 27. If needed, have business associate contracts been signed by all parties to the Physician Contract?
- Yes No 28. Has a legal firm reviewed this specific contract?
Name of legal firm that reviewed contract: _____
- Yes No 29. Was an approved Hospital template used to create this Physician Contract?

[NB: Lease Contracts ignore questions 10, 16, 19, 21, 22, 23 and 24 which do not apply or are covered by Appendix B.]

in approval

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance: 51.00 Physician Financial Arrangements - Review and Approval

Contract Certification

I, _____ of El Camino Hospital hereby certify that to the best of my knowledge,
(responsible party negotiating)

the following matters are true for the attached contract by and between El Camino Hospital and _____

(Physician) dated _____ (the "Arrangement").

- 1) There are no other arrangements, written or oral with the physician except set forth in the Arrangement;
- 2) No payment has been or will be made to the physician referenced herein outside of the terms and condition of the arrangement unless such outside payment is also consistent with El Camino Hospital's policies;
- 3) The contract is in compliance with Administrative Policy 51.00 guidelines.
- 4) All of the statements above and in the Compliance Checklist are complete and correct.

Date: _____

Signature: _____
(Hospital responsible party negotiating)

in approval

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance:51.00 Physician Financial Arrangements - Review and Approval

CATEGORY: Administrative
LAST APPROVAL DATE:

APPENDIX C

Lease Contract Review Checklist

- Yes ___ No ___ 1. Is the term of the Physician Lease Contract for at least one year?
- Yes ___ No ___ 2. Does the Physician Lease Contract describe what is being leased and all services that will be included?
- Yes ___ No ___ 3. Are the costs of Tenant Improvements incorporated into the Physician Lease Contract?
- Yes ___ No ___ 4. Have fair-market value (FMV) rates been determined based at time of signing? [The Physician Lease Contract
- Yes ___ No ___ 5. Does the lease rate include an inflator value for future FMV?
- Yes ___ No ___ 6. Is Physician using the space now?
- Yes ___ No ___ 7. Will all applicable property taxes be paid by the Physician under the Physician Lease Contract?
- Yes ___ No ___ 8. Were any loans or loan guarantees made to the Physician?
- Yes ___ No ___ 9. Was the Hospital template used to create this Physician Lease Contract?
- Yes ___ No ___ 10. Were any of the terms modified? If yes, attach a copy marked to show changes.
- Yes ___ No ___ 11. Within 5 days after final execution, the Physician Lease Contract must be forwarded for scanning into Meditract.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.



POLICY/PROCEDURE TITLE: Corporate Compliance:51.00 Physician Financial Arrangements - Review and Approval

**APPENDIX D
FORM OF PHYSICIAN MONTHLY TIME**

in approval

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the electronic version prevails.

ECH BOARD COMMITTEE MEETING AGENDA ITEM COVER SHEET

Item:	Proposed FY18 Committee Goals Corporate Compliance/Privacy and Internal Audit Committee May 18, 2017
Responsible party:	Diane Wigglesworth, Sr. Director, Corporate Compliance
Action requested:	For Possible Motion (recommendation to the Governance Committee for approval)
Background:	Each Board Advisory Committee recommends committee goals for itself for the next fiscal year; the Governance Committee reviews all goal recommendations and then recommends the full set of goals to the Hospital Board for approval.
Other Board Advisory Committees that reviewed the issue and recommendation, if any:	None.
Summary and session objectives:	To review proposed goals and advise if changes are recommended.
Suggested discussion questions:	None.
Proposed Committee motion, if any:	To recommend that the Governance Committee recommend approval of the Compliance Committee's FY18 proposed goals.
LIST OF ATTACHMENTS:	<ol style="list-style-type: none"> 1. Proposed FY18 Compliance Committee Goals

Corporate Compliance/Privacy and Audit Committee

Proposed Goals FY18

Purpose

The purpose of the Corporate Compliance/Privacy and Audit Committee (“Compliance and Audit Committee”) is to advise and assist the El Camino Hospital (ECH) Hospital Board of Directors (“Board”) in its exercise of oversight by monitoring the compliance policies, controls and processes of the organization and the engagement, independence and performance of the internal auditor and external auditor. The Compliance and Audit Committee assists the Board in oversight of any regulatory audit and in assuring the organizational integrity of ECH in a manner consistent with its mission and purpose.

Staff: Diane Wigglesworth, Sr. Director of Corporate Compliance

The Sr. Director, Corporate Compliance shall serve as the primary staff support to the Committee and is responsible for drafting the Committee meeting agenda for the Committee Chair’s consideration. Additional members of the executive team or outside consultants may participate in the Committee meetings upon the recommendation of the Sr. Director, Corporate Compliance and at the discretion of the Committee Chair.

Goals	Timeline by Fiscal Year (Timeframe applies to when the Board approves the recommended action from the Committee, if applicable.)	Metrics of Success Achieved
<ul style="list-style-type: none"> ▪ Review and evaluate Hospitals plan for IT Security Awareness Training for organization 	<ul style="list-style-type: none"> ▪ Q1 FY18 	<ul style="list-style-type: none"> ▪ Committee reviews plan
<ul style="list-style-type: none"> ▪ Review and evaluate Hospital’s policy and education plan regarding responding to government investigations 	<ul style="list-style-type: none"> ▪ Q1 FY18 	<ul style="list-style-type: none"> ▪ Committee reviews policy and plan.
<ul style="list-style-type: none"> ▪ Review status of HIPAA Readiness 	<ul style="list-style-type: none"> ▪ Q2 and Q4 FY18 	<ul style="list-style-type: none"> ▪ Committee reviews status
<ul style="list-style-type: none"> ▪ Review and evaluate Managements recommended ERM framework regarding how the Board will establish it’s risk appetite and risk tolerance levels 	<ul style="list-style-type: none"> ▪ Preliminary report in Q3 FY18 and final recommendations in Q4 FY18 	<ul style="list-style-type: none"> ▪ Committee reviews framework recommendations.

Submitted by:

John Zoglin, Chair, Corporate Compliance/Privacy and Audit Committee

Diane Wigglesworth, Executive Sponsor, Corporate Compliance/Privacy and Audit Committee



AUDIT ENTRANCE

El Camino Healthcare District

MAY 18, 2017

MOSS-ADAMS LLP

Certified Public Accountants | Business Consultants



Audit and Compliance Committee

El Camino Healthcare District

Dear Committee Members:

Thank you for your continued engagement of Moss Adams LLP, the provider of choice for healthcare organizations. We are pleased to present our audit plan for El Camino Healthcare District for the year ending June 30, 2017. We would also like to discuss current-year developments and auditing standard changes that will affect our audit.

We welcome any questions or input you may have regarding our audit plan, and we look forward to working with you.

Your Dedicated Team



Brian Conner
Partner



Joelle Pulver
Partner



Jennifer Sattavorn
Audit Manager



Katherine Djiauw
Audit Senior Manager

Required Communications to those Charged with Governance

- Auditor's responsibility under U.S. auditing standards
 - Planned scope and timing of audit
-
- Significant audit findings
 - Qualitative aspects of accounting practices
 - Difficulties encountered in performing the audit
 - Corrected and uncorrected misstatements
 - Management representations
 - Management consultations with other independent accountants
 - Other audit findings or issues



Our Responsibility Under US Generally Accepted Auditing Standards

1 To express our opinion on whether the consolidated financial statements prepared by management with your oversight are fairly presented, in all material respects, in accordance with U.S. GAAP. However, our audit does not relieve you or management of your responsibilities.

2 To perform an audit in accordance with generally accepted auditing standards issued by the AICPA, and the California Code of Regulations, Title 2, Section 1131.2, State Controller's *Minimum Audit Requirements* for California Special Districts and design the audit to obtain reasonable, rather than absolute, assurance about whether the consolidated financial statements are free of material misstatement.

3 To consider internal control over financial reporting as a basis for designing audit procedures but not for the purpose of expressing an opinion on its effectiveness or to provide assurance concerning such internal control.

4 To communicate findings that, in our judgment, are relevant to your responsibilities in overseeing the financial reporting process. However, **we** are not required to design procedures for the purpose of identifying other matters to communicate to you.

Audit Process

INTERNAL CONTROLS

- Includes Information Technology



ANALYTICAL PROCEDURES

- Revenues and expenses
- Trends, comparisons, and expectations

SUBSTANTIVE PROCEDURES

- Confirmation of account balances
- Vouching to supporting documentation
- Representations from attorneys and management
- Examining objective evidence

What is Materiality?

It's the amount of a misstatement that could influence the economic decisions of users, taken on the basis of the consolidated financial statements

It's calculated using certain **quantitative** (*e.g., total assets*) and **qualitative** factors (*e.g., covenants, expectations, or industry factors*)



It's used to identify :

- Significant risk areas
- Nature, timing, extent, and scope of test work
- Findings or misstatements

Significant Audit Areas



Net Patient Accounts Receivable and Revenue



Pension



Long-Term Debt



Fixed Assets

Consideration of Fraud



Auditors must consider fraud to
“improve the likelihood that auditors will detect material misstatements due to fraud in a financial statement audit.”

How we gather information to identify fraud-related risks of material misstatement:

- Brainstorm with team
- Conduct personnel interviews
- Document understanding of internal control
- Consider unusual or unexpected relationships identified in planning and performing the audit

Procedures to be performed:

- Examine general journal entries for nonstandard transactions
- Evaluate policies and accounting for revenue recognition
- Test and analyze significant accounting estimates for biases
- Evaluate the business rationale for significant unusual transactions

Deliverables



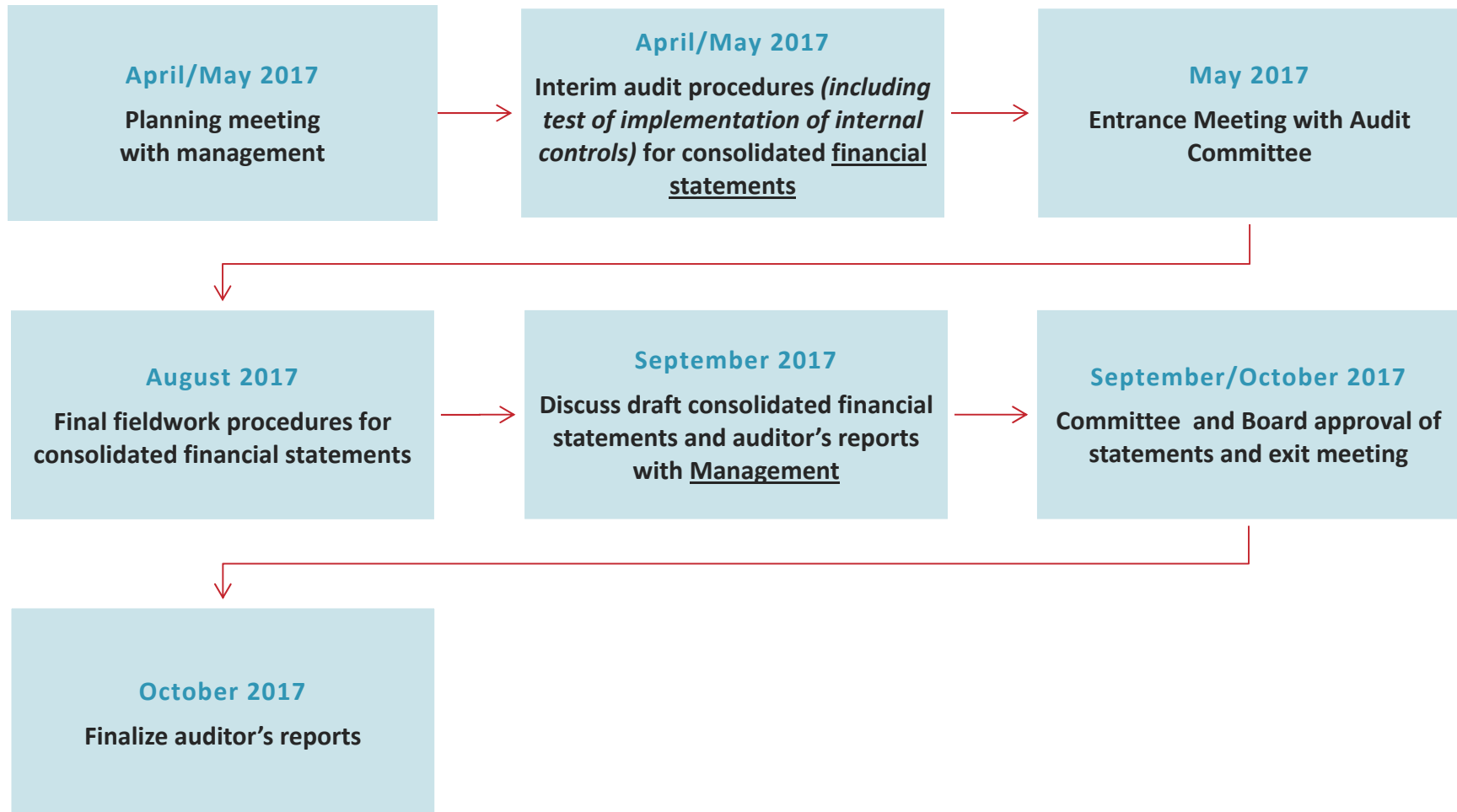
We will issue the following reports:

- Audit report on the consolidated financial statements of El Camino Healthcare District as of and for the year ending June 30, 2017
- Audit report on the financial statements of El Camino Foundation as of and for the year ending June 30, 2017
- Audit report on the financial statements of CONCERN: EAP as of and for the year ending June 30, 2017
- Audit report on the financial statements of Auxiliary as of and for the year ending June 30, 2017
- Report to Those Charged with Governance (Communicating required matters and other matters of interest)
- Report to Management and the Audit and Compliance Committee (Communicating Internal Control Related Matters Identified in an Audit)

We have also been engaged to perform the following nonattest services:

- Assist in the drafting of the consolidated financial statements

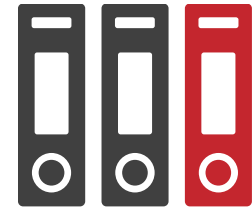
Audit Timing





Accounting Update

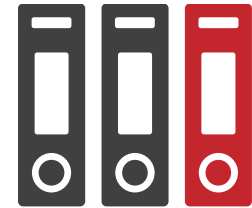
New Standards



GASB 74 / 75 | Financial Reporting for Postemployment Benefits Other than Pension Plans (OPEB)

- Effectively replaces GASB 43 and 45.
- Reporting essentially the same as pensions under GASB 67 and 68, respectively. Significant note disclosure and required supplementary information.
- Effective for OPEB plan annual periods beginning after June 15, 2016, and Employers for annual periods beginning after June 15, 2017.

New Standards



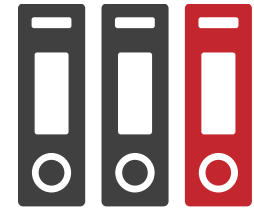
GASB 76 | The Hierarchy of GAAP for Governments

- Establishes two categories:
 - Category A: Formally approved statements by the GASB Board.
 - Category B: GASB Technical Bulletins and Implementation Guides.
- Effective for annual periods beginning after June 15, 2016.

GASB 77 | Tax Abatement Disclosures

- Occurs when a government promises to forego tax revenue and second entity promises to take action to contribute to the economic development or otherwise benefit citizens of the foregoing government.
- Effective for annual periods beginning after June 15, 2016.

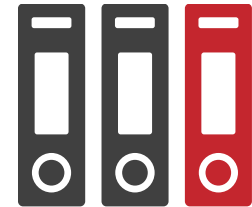
New Standards



GASB 80 | Blending Requirements for Certain Component Units—an amendment to GASB 14

- Permits blending of a not-for-profit organization (which may be legally separate and have their own board) if the primary government is the sole corporate member.
 - This standard was established specifically because it was already common practice among healthcare entities.
- Effective for annual periods beginning after June 15, 2016.

Exposure Drafts



Leases

- Would treat all leases as financings (no classification of capital vs. operating) similar to FASB ASU 2016-02.
- Includes non-cancellable period + periods covered by options to renew if reasonably certain to be exercised.
- Lessee would record an intangible asset (amortized over the shorter of its useful life or lease term) and present value of future lease payments as a liability.
- Lessor would record a lease receivable and deferred inflow of resources for cash received up front + future payments (revenue recognized over lease term in a systematic and rational basis).
- Final statement expected in late 2016 or early 2017.



About Moss Adams

MOSS ADAMS_{LLP}
Certified Public Accountants | Business Consultants

Keeping You Informed



Keeping you informed about changes in the financial landscape is one of our top priorities. We closely monitor regulatory agencies, participate in industry and technical forums, and write about a wide range of general as well as industry-specific accounting, tax, and business issues. The goal? To provide you with actionable information and guidance to help your organization succeed.

Continuing education is vitally important to us, and we're happy to share our knowledge with you and your staff. We frequently offer a wide range of topical online seminars, many of which are archived and available on demand, allowing you to watch them on your schedule.



Our Services for Healthcare Organizations

ASSURANCE

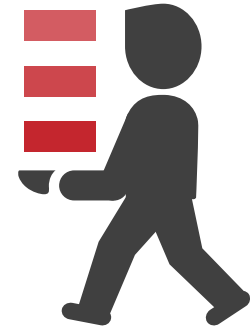
- Agreed-upon procedures
- [Audits and reviews](#)
- Single audits
- Compliance examinations pursuant to federal reporting requirements
- [Employee benefit plan services](#)
- Written acknowledgments and agreed-upon procedure engagements in connection with tax-exempt bond offerings

GENERAL CONSULTING

- [Fraud investigation and forensic accounting](#)
- [IT consulting](#)
- [Strategic business planning](#)
- [Sustainability services](#)
- [Wealth services](#)


HEALTHCARE CONSULTING

- ACOs and integrated delivery models
- 5010 readiness
- ICD-10 road map
- Chargemaster management
- Claims review and processing
- Coding and chart reviews
- Contract review
- Data analytics
- Dependent care audits
- Financial modeling and forecasting
- Hospital feasibility studies
- Litigation support
- Managed care operations
- Practice operation assessments
- Process improvement
- Regulatory compliance
- Reimbursement services
- Revenue cycle assessments
- Revenue recovery and enhancement
- Strategic planning




Moss Adams by the Numbers

Health Care Group



2,200+ clients
across the nation

 30 practice partners

 250+ professionals

HEALTH CARE CLIENTS
in the Western United States

Our team of dedicated professionals has served clients across the health care continuum for 38 years.



2,200
hospitals, health systems,
independent practices,
care centers, and more

MOSS ADAMS
By the Numbers




clients in every state
across the nation

103 countries served
via *Praxity AISBL*

 527 million
dollars in revenue

 104 years
in business

 30+ industries
served

 28 locations
across the nation

 280+ partners

 6:1 staff-to-partner
ratio

Brian Conner

Brian.Conner@mossadams.com

(209) 955-6114

Joelle Pulver

Joelle.Pulver@mossadams.com

(415) 677-8291





El Camino Hospital[®]

THE HOSPITAL OF SILICON VALLEY

Cybersecurity Threats and Risks

Diane Wigglesworth,
Sr. Director, Corporate Compliance

May 18, 2017

Healthcare Cybersecurity Facts: 2016 in Review

The techniques, tools, and tactics used by cybercriminals are changing at an exponential rate, as is the scope of those attacks.

- 27%** of all reported breaches were in the Healthcare Industry (Healthcare was the most attacked industry from January to June 2016)
- 48%** of successful healthcare attacks were due to injecting malicious software
- 63%** increase in breaches over 2015 (93 breaches / 12,057,759 records)
- 200%** increase in HIPAA reportable data breaches since 2014
- 31%** of HIPAA data breaches were caused by IT/Hacking
- 300%** increase in Ransomware occurrences between Jan.2015 and Mar.2016
- 655,000** health records were offered for sale on the dark web in June 2016

Why Healthcare?

- **Financially Lucrative:** cybercrime was expected to generate **\$600 billion** in revenue in 2016
 - Healthcare information is worth 10 times that of credit card numbers on the black market
- **Easy:** High possibility of success with little risk
- **Target Rich:** Medical devices (e.g., radiology/dialysis/therapeutic/life support devices), Hardware (e.g., computers/phones/routers/firewalls), EHR Software, Financial/Employee information, Building Control & Plant Operating Systems are all targets for cyber crime
- **Quick Payout:** Paying ransom for stolen records for some is considered the quickest and easiest way to protect patients and the healthcare entity
 - Loss of control of these records can lead to risks to patient care, employees, and building safety. There can also be a loss of community trust, a decrease to entity reputation, and monetary loss due to fines and possible decrease in patient census.
- **Potential for Fraudulent CMS Claims:** Theft of PHI provides the basis for easy submission of fraudulent claims to CMS

Emerging Cybersecurity Threats For Hospitals

- **Malware:** Malicious software that sneaks into the network through encrypted traffic
- **Ransomware:** Locks users out of data or networks until payment of ransom
- **Phishing Attacks:** Often come through e-mails or attachments
- **Man in the middle (MITM) attacks:** Malware sits on the computer and waits for credentials then swaps out the server that receives the communication
- **Targeting employees to compromise corporate networks:** Employees download or use software without IT consent or by opening emails from unknown senders
- **Medical Devices:** Difficult to detect and mediate attacks on devices

Healthcare Data Breaches in the News *(last 6 months)*

- **July 2016** - \$2.75m settlement with Mississippi Medical Center (UMMC)
 - Had been aware of risk and vulnerabilities to systems since 2005 yet no significant risk management activity occurred until after a laptop was stolen in 2013, affecting 10K individuals.
- **August 2016** - \$5.55m settlement with Advocate Health Care, IL
 - Noncompliance with Security Rule; 4 million records impacted.
- **Nov. 2016** - \$650K settlement with University of Massachusetts
 - Malware infection on work station of university language center.
- **Jan. 2017** - \$475K settlement with Presence Health, IL.
 - Untimely reporting of a breach of unsecured PHI.
- **Feb. 2017** - \$5.5m settlement with Memorial Healthcare Systems
 - Employee accessed 115,143 patients without detection for 1 year.

What Have We Learned?

- Healthcare is a highly targeted industry
- Attacks are targeted, sophisticated, and widespread
- Employee's need more awareness training
- Vendors/Business Associates can put the organization at risk
- Annual Security Risk Assessments and implementation of resulting mitigation plans are vital
- Most healthcare institutions cannot detect attacks
 - Many attacks go undetected for considerable periods of time, an estimated 280 days on average

Cybersecurity Measures in Use (Based on 2016 AHA Survey)

Cybersecurity Measure	Share of Surveyed Hospitals Implementing Measure (2,146)			
	ECH	<90%	<80%	<70%
Unique ID of system users	●	●		
Automatic logoff of system users	●	●		
Required use of strong passwords	●	●		
Passcodes for mobile devices		●		
Use of intrusion detection systems	●		●	
Encryption of wireless networks	●		●	
Encryption of laptops and/or workstations	●	●		
Encryption of removable storage media	●		●	
Encryption of mobile devices			●	
Mobile device data wiping			●	
At least annual risk analysis to identify compliance gaps and security vulnerabilities	●	●		
At least annual infrastructure security assessment	●	●		
Security incident event management	●			●

Top Cybersecurity Compliance Risks and Recommended Actions to Moderate those Risks

Risks	Requirements / Actions
<p>Incomplete/Inaccurate Risk Assessment: Organizations often underestimate the amount of ePHI within their environment</p>	<ul style="list-style-type: none"> • Conduct accurate, thorough assessment of potential risks to confidentiality/availability of ePHI held by ECH. • Consider applications (e.g., EHR, Billing, PM, documents, spreadsheets, all servers, etc.), computers, medical devices, messaging apps, mobile devices, copiers/printers, media (e.g., CDs, drives, etc.).
<p>Lack of Business Associate Agreements: HIPAA requires entities & business associates to enter into agreements to ensure business associates will safeguard PHI</p>	<p>Examples of Business Associates with access to PHI include:</p> <ul style="list-style-type: none"> • Collection agencies, attorneys, independent medical transcriptionists • Subcontractors providing remote backup services of PHI data for an IT-contractor-business associate of a health care provider
<p>Insider Threat: Organizations must implement policies & procedures ensuring employees have appropriate access (or not) to PHI</p>	<ul style="list-style-type: none"> • Workforce screening procedures (background checks) should be included in the hiring process. • The termination process should include revocation of PHI access.
<p>Insufficient Data Backup & Contingency Planning: Organizations must ensure adequate contingency plans are in place & would be effective in event of disaster or emergency</p>	<ul style="list-style-type: none"> • Leveraging the resources of cloud vendors may aid with plans re: applications or computer systems. • As reasonable and appropriate, entities must periodically test their plans and revise them as necessary, depending on identified deficiencies.

Top Cybersecurity Compliance Risks and Recommended Actions to Moderate Those Risks *(cont.)*

Risks	Requirements / Actions
<p>Failure to Manage or Mitigate Identified Risk: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level</p>	<p>OCR Investigations revealed instances of breaches due to vulnerabilities that had been previously identified during risk analysis. Proposed security measures (often including implementation of encryption) had not been implemented within the timeframe noted in the Remediation Plan.</p>
<p>Lack of Appropriate Auditing: HIPAA requires the implementation of hardware, software, &/or procedures that record and examine info system activity that contain or use ePHI</p>	<p>Once appropriate audit mechanisms are put in place, procedures must be implemented to, “regularly review records of information system activity, such as audit logs, access reports, & security incident tracking reports”. Metrics to track:</p> <ul style="list-style-type: none"> • Access during non-working hours, access to abnormally high number of records containing PHI, access to PHI of persons for which media interest exists, access to PHI of employees
<p>No Patching of Software: The use of unpatched or unsupported software could introduce additional risk to the environment</p>	<ul style="list-style-type: none"> • Audit operating systems, EMR/PM, productivity software, router/firewall firmware, antivirus/malware, multimedia runtime environments (e.g., Adobe, Flash, Java), etc. • Continued use of such systems must be included in risk analysis, along with implementation of appropriate mitigation strategies, to reduce risk to reasonable/acceptable levels.
<p>Improper Disposal: Entities must implement policies and procedures to ensure that electronic media which may contain ePHI is disposed of in a secure manner</p>	<ul style="list-style-type: none"> • The procedures must ensure that electronic media have been cleared, purged, or destroyed consistent with NIST guidelines, such that the data cannot be retrieved. • These media must be disposed of in a timely manner. • Secure disposal includes non-computer devices (e.g., printers/copiers systems, medical devices).

Next Steps

The Privacy and Security Rule applies to all aspects of a covered entity's operations, including potential business expansion, when other provider's records come into the covered entity's possession.

1. Risk analyses of HIPAA covered entities and their business associates must be undertaken to understand the threats and vulnerabilities to individuals' data, and to have appropriate safeguards in place to protect this information. Findings of the analyses must be addressed in a timely manner.
2. Keep up with the technology, at least to the extent of using readily available patches and supportable software.
3. Protecting paper PHI still matters.
4. Stringently implement and enforce security policies. ENCRYPT, ENCRYPT, ENCRYPT.

Next Steps *(continued)*

5. Train thoroughly and often, utilizing different educational platforms (include random testing of staff).
6. Senior leadership must help to define the culture of the organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected.
7. Test Incident Response plans. Revise plans in a timely manner to address identified deficiencies.

ECH BOARD COMMITTEE MEETING AGENDA ITEM COVER SHEET

Item:	Key Performance Indicators Corporate Compliance/Privacy and Internal Audit Committee May 18, 2017
Responsible party:	Diane Wigglesworth, Sr. Director, Corporate Compliance
Action requested:	For Information
Background:	Key performance indicators were developed to track required elements from the Federal Sentencing Guidelines. These indicators help the Committee monitor activity and review organizational trends.
Other Board Advisory Committees that reviewed the issue and recommendation, if any:	None.
Summary and session objectives:	To review the trending of key indicators. Compliance investigated a number of concerns identified during chart audits regarding billing integrity and identified corrections that were needed. Corrective actions and additional education to staff regarding charting was implemented. The total number of regulatory and privacy breaches requiring reports to CDPH continues to trend down compared to previous years.
Suggested discussion questions:	1. Are there any trends of concern?
Proposed Committee motion, if any:	None. This is an informational item.
LIST OF ATTACHMENTS:	1. Corporate Compliance Scorecard 2. KPI 2-year Trend Graph

Corporate Compliance Scorecard FY17

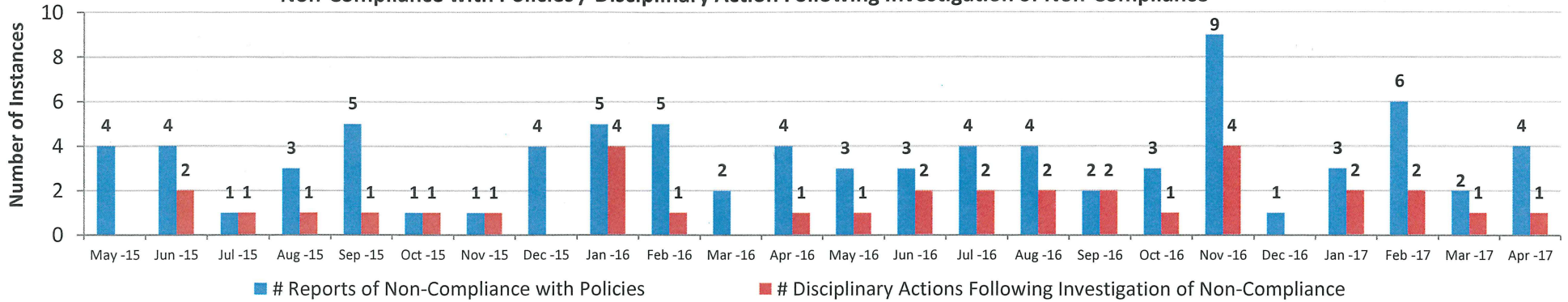
El Camino Hospital

Key Performance Indicator	FY17 Current Month	Current YTD Actual	Prior YTD Actual
Total Number of Hospital Discharges (excluding normal newborn)	1,697	14,327	13,980
Core Elements			
Policies and Procedures			
	Apr. 2017	Jul - Apr FY17	Jul - Apr FY16
Number of reported instance when policies not followed	4	38	25
Number of disciplinary actions due to Investigations	1	17	10
Education and Training			
	Apr. 2017	Jul - Apr FY17	Jul - Apr FY16
Percentage of new employees trained within 30 days of start date	100%	100%	100%
Investigations			
	Apr. 2017	Jul - Apr FY17	Jul - Apr FY16
Total number of investigations	25	232	154
Investigations open	1	1	0
Investigations closed	24	231	154
Hotline concerns substantiated	1	16	15
Hotline concerns not substantiated	4	17	18
Average number of days to investigate concerns	7	7	6
Reporting Trends			
	Apr. 2017	Jul - Apr FY17	Jul - Apr FY16
Anti-Kickback/Stark	8	52	29
EMTALA	1	2	4
HIPAA Reports	12	135	128
HIPAA Security Breaches	1	4	3
Billing or Claims	4	73	61
Conflict of Interest	1	9	3
Reported Events to CMS			
	Apr. 2017	Jul - Apr FY17	FY16 Actual
Number of total events self reported by ECH	0	0	0
Number of self reported events followed up by CMS	0	0	0
CMS initiated visits (separate from ECH self reported events)	0	0	0
Number of statement of deficiencies issued to ECH	0	0	0
Number of Actual Sanctions, fines or penalties	0	0	0
Reported Events to CDPH			
	Apr. 2017	Jul - Apr FY17	FY16 Actual
Number of total regulator events self reported by ECH	0	5	11
Number of self reported events followed up by CDPH	0	5	5
Number of total privacy breaches self reported by ECH	1	13	18
CDPH initiated visits (separate from ECH self reported events)	0	7	7
Number of statement of deficiencies issued to ECH	0	0	3
Number of Actual/Realized Sanctions, fines or penalties	0	0	0
Monitoring and Audit Findings			
	Apr. 2017	Jul - Apr FY17	FY16 Actual
Total number of Audit Findings	3	39	47
Number of findings identified has high severity	0	11	6
Monitoring and Audit Findings			
	Apr. 2017	Jul - Apr FY17	FY16 Actual
Number of Open Liability Claims	7	7	10
Number of Open Liability Lawsuits	9	9	7

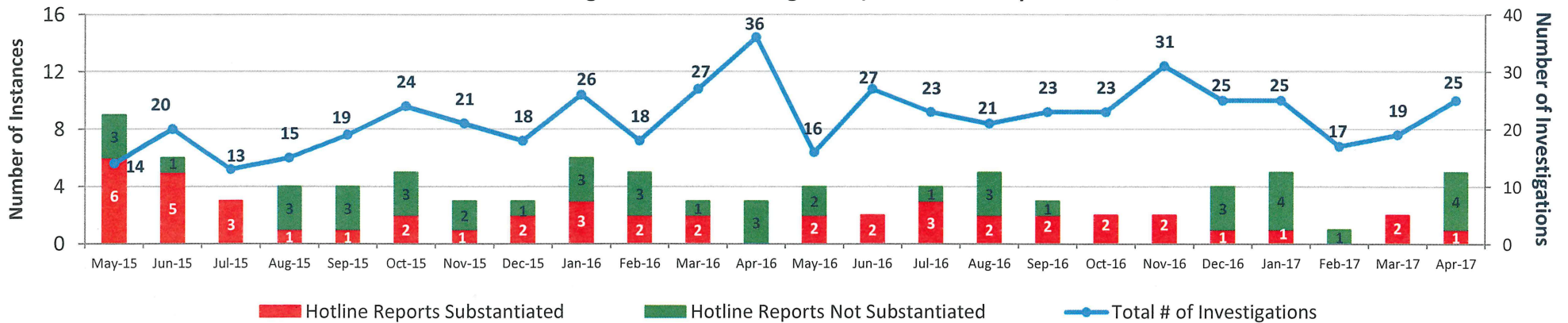
Corporate Compliance

Policies & Procedures

Non-Compliance with Policies / Disciplinary Action Following Investigation of Non-Compliance



Investigations: Total Investigations / Hotline Activity



Privacy Breaches Requiring Report to Outside Entity

