Mayers Memorial Hospital District

Chief Executive Officer

Matthew Rees, MBA

Board of Directors

Allen Albaugh, President
Brenda Brubaker, Vice President
Abe Hathaway, Treasurer
Michael D. Kerns, Secretary
Art Whitney, Director

BOARD of DIRECTORS MEETING AGENDA

August 27, 2014, 1:00 PM
Board Room (Burney)

Mission Statement

Mayers Memorial Hospital District serves the Intermountain area providing outstanding patient-centered healthcare to improve quality of life through dedicated, compassionate staff and innovative technology.

1	**CALL MEETING TO ORDER – Allen Albaugh, President**	
2	**CALL FOR REQUEST FROM THE AUDIENCE: PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS:** Persons wishing to address the Board are requested to fill out a "Request Form" prior to the beginning of the meeting (forms are available from the Clerk of the Board (M-W), 43563 Highway 299 East, Fall River Mills, or in the Board Room). If you have documents to present for the members of the Board of Directors to review, please provide a minimum of nine copies. When the President announces the public comment period, requestors will be called upon one-at-a time, please stand and give your name and comments. Each speaker is allocated five minutes to speak. **Comments should be limited to matters within the jurisdiction of the Board.** Pursuant to the Brown Act (Govt. Code section 54950 et seq.) **action or Board discussion cannot be taken** on open time matters other than to receive the comments and, if deemed necessary, to refer the subject matter to the appropriate department for follow-up and/or to schedule the matter on a subsequent Board Agenda.	
3	**APPROVAL OF MINUTES:** 3.1 Regular Meetings – July 30, 2014 **(ATTACHMENT A)**	***ACTION ITEM***
4	**OPERATIONS** ▸ C3 Report (CEO, CNO, CCO) **(ATTACHMENT B)** ▸ Facilities Management Report – Louis Ward, Director of Support Services ▸ Support Services Report/EMR Report by Louis Ward, Director of Support Services	Information
5	**REPORTS** **5.1 Surgery Department Update –** Lisa Akin, Surgery Department Manager..... **5.2 Workers Comp Quarterly Report** – Travis Lakey..... **5.3 Safety Quarterly Report** - Louis Ward.....	Information
6	**BOARD COMMITTEES:** **6.1 Finance Committee – Chair Allen Albaugh** 6.1.1 Committee Meeting Report 6.1.2 July 2014 Financial review and acceptance of financials (*dispersed separately*)..... 6.1.3 BOD Quarterly Finance Review (Binders)..... 6.1.4 USDA Loan Resubmission Review and Approval (if needed)..... **6.2 Strategic Planning Committee – Chair Abe Hathaway** 6.2.1 Committee Meeting Report **6.3 Quality Committee – Chair Brenda Brubaker** 6.3.1 Committee Meeting Report 6.3.2 Approval of HIPPA Policy – Employee Handbook Privacy & Security section **(Attachment C)**...	 Information ***ACTION ITEM*** ***ACTION ITEM*** ***ACTION ITEM*** ***ACTION ITEM***

7	**NEW BUSINESS** 7.1 Fire panel Update and possible purchase approval (Ward).....	***ACTION ITEM***
8	**8.1 INFORMATION/REPORTS/BOARD EDUCATION/ANNOUNCEMENTS** ▶ Board Education – QHR Webinar 2nd Tuesdays 2014, 10 a.m.	Information/ discussion
9	**ANNOUNCEMENT OF CLOSED SESSION:** 9.1 **Government Code Section 54962** Quality Assurance: Quality Improvement Issues, Medical Staff Report (Dr. Dan Dahle, Chief of Staff) 9.2 **Government Code Section54957: Personnel** 9.2.1 CEO Bonus Criteria..... 9.2.2 CEO Evaluation..... 9.3 Reappointment..... ✓ Dan Dahle, MD - reappointment 9.4 **Approve minutes of the July 30, 2014** Closed Session minutes.....	***ACTION ITEM*** ***ACTION ITEM***
9	**RECONVENE OPEN SESSION: REPORT ACTIONS TAKEN DURING CLOSED SESSION**	
10	**ADJOURNMENT:** Next Regular Meeting September 24, 2014 – Fall River Mills, CA	

Public records which relate to any of the matters on this agenda (except Closed Session items), and which have been distributed to the members of the Board, are available for public inspection at the office of the Clerk to the Board of Directors, 43563 Highway 299 East, Fall River Mills CA 96028.

This document and other Board of Directors documents are available online at www.mayersmemorial.com.

Posted/Distributed: 08/21/14

Attachment A
DRAFT

Mayers Memorial Hospital District
Board of Directors – Regular Board Meeting

Date: July 30, 2014
Time: 1:01 P.M.
Location: Mayers Memorial Hospital
Fall River Mills, California

(These minutes are not intended to be a verbatim transcription of the proceedings and discussions associated with the business of the board's agenda; rather, what follows is a summary of the order of business and general nature of testimony, deliberations and action taken.)

1. CALL MEETING TO ORDER: President Allen Albaugh called the regular meeting to order at 12:59 p.m. on the above date with the following present:

Allen Albaugh, President
Brenda Brubaker, Vice President
Mike Kerns, Secretary
Abe Hathaway, Treasurer
Art Whitney, Director

Board Members Absent: none
Staff Present: Matt Rees, CEO; Keith Earnest, CCO; Sherry Wilson, CNO; Valerie Lakey, Board Clerk; Travis Lakey, CFO; Louis Ward, Director of Support Services; Caleb Johnson, Compliance

2. CALL FOR REQUEST FROM AUDIENCE TO SPEAK TO ISSUES OR AGENDA ITEMS: None

3. APPROVAL OF MINUTES – *A motion/second (Kerns/Whitney), and carried, the Board of Directors accepted the minutes for the regular meeting – June 25, 2014.*

4. OPERATIONS REPORT:

In addition to the written operations report included in the board packet, the following verbal reports and discussions are summarized below:

- ***Matt Rees, CEO:*** Rees reviewed his submitted written report. One of the highlights was that Dr. Syverson will be working soon. Albaugh noted that he wants to track the financials on surgery in a spreadsheet form to be evaluated in 6 months (December 2014) Lisa Akin will present a department report at the August meeting.

- ***Keith Earnest, CCO:*** In addition to the submitted report, Earnest reported:

  - Imaging – With the PACS system we have been at an impass with the images held by the previous company. They do not want to release them. Dr. Halt has helped us with this situation. We are making progress. We have legal counsel working on it.

  - Pharmacy – after hours Pharmacy Company we have been using is out of business – Earnest will be processing in the interim until August 13th when the new company starts. Whitney had a lot of questions about the remote verification company. The new company waived the set-up fee of $8000.

  - Skilled Nursing label meets the state standard. Acute labels are handwritten – new legislation could make that a liability.

  - PT referrals have dropped – since Dr. Godzich has left. Dr. Dahle said physicians are seeing patients less often.

  - Mary Ranquist is taking over as Hospice manager – Earnest will report to the board.

- ***Sherry Wilson, CNO:*** In addition to the submitted report, Wilson reported on the following:
  - Census is at 74.
  - We have been getting a lot of Partnership short-term rehab patients – need to look at the details of billing (patients out of swing bed days) We have only have been accepting patients within our district. Dr. Watson is the final say on admitting the patients. It is helping to fill some of our beds.
  - We had our survey last week – it went well. There was a big difference in the survey team this year. They focused on psychotropic's – we have a higher average – we are at 35% - they would like to see around 17%. We are waiting for the report. We had NO med errors.
  - Alzheimer's – Dementia patients – they want us to reduce psychotropic's, which creates a potential harm to staff – Whitney says there is a protocol to follow to remove potentially dangerous patients.
  - Wilson, Dr. Watson and staff will be visiting another facility to get some ideas.

- ***EMR – Louis Ward, Director of Support Services***

Dave Burks is new maintenance lead. The staff is trying to develop a collaborative environment. There have been several things that have stemmed from the survey and has prompted the development of a maintenance plan for both facilities (general and regular maintenance tasks). There will be a plan with quarterly, semi-annual and annual tasks. This will be a part of the POC.

- We are awaiting Fire –Life Safety survey. Working to prepare for that.
- Support Services – Inventory at FY – only off by $470. We do regular counts during the year – discrepancies go to appropriate department.
- Dietary – electronic charting – Aug 15, 2014 – Acute side Dietician will review.
- Environmental services – Aramark linen service – expected $80,000 savings per year.
- IT – PACS – legal issues – we are moving forward with interfaces, vitals
- We continue to work on HIE – Northstate health connect – how to manage population health in the northstate region.
- MVHC – MMHD collaborative meetings – 3rd meeting in August – items: shared patient portal, referral process, swing patients
- Documents have been sent to CMS for stage 1 year 2
- ICD 10 – will be October 2015

- Paper usage – is down, we recently purged all of the old records (500 boxes). We are working with a company with for cloud based recovering. We have tape back-up and ICE back-up

5. BOARD COMMITTEES:

5.1 Finance Committee – Chair Allen Albaugh

5.1.1 Committee meeting report – see finance meeting minutes

- Albaugh would like to look into the possibility of a well/pump for irrigation and fire suppression.
- Albaugh also noted that he heard rumor of the LTC facility in Weed closing. Wilson will check into it.

5.1.2 June 2014 and FY14 year end financial Reports ***(Kerns/Hathaway) Approved (All)***

- Financials – Discussed yearend report
- Working on reducing expenses
- Auditors on-site in September
- Conservative on cost report estimate

5.1.3 Health Insurance recommendation and approval of Resolution 2014-5 to leave CalPers as of December 31, 2014. Decision on specific plan will be made in September. Insurance and Employee Benefits Committee will continue to meet.
(Kerns/Hathaway) Approved (All)

5.1.4 USDA Loan Resubmission – No action taken as we have not heard anything from the State USDA department. It was decided to delay the discussion until we hear back from State. At that time the Board will have to approve the application before it is sent to federal level.

It was noted that we have looked at a few other options as a back-up plan and Albaugh suggested to keep exploring options in the meantime.

5.2 Strategic Planning Committee – Chair Abe Hathaway

5.2.1 Committee Meeting Report – Hathaway reported on the July Committee meeting. Minutes were sent out to all board members. Highlights included:

- Website review
- Orthopedics and surgery updates
- Whitney mentioned that we should look into a Coumadin and Diabetic clinic – there will be some good possibilities for reimbursement forthcoming.

5.3 Quality Committee – Chair Brenda Brubaker

5.3.1 Committee Meeting Report: Quality Committee meeting. Brubaker referenced the committee meeting minutes that were sent out and noted that the "clean claim" percentage form the business office was a highlight of the department presentations.

6. NEW BUSINESS

6.1 Policies and Procedures –The following P & P's were presented to and approved by the board. Brubaker had concern that some of the policies do not need to go to the board for approval. It was noted the software is new and being fine-tuned. There are still some things to work out, but overall we are making good progress and keeping up on policies.

- Pressure Ulcer Turn Clock
- Request to Be Cleared for Scheduling MMH493
- Cancellation of Purchase Orders
- Communications
- Construction Purchase Orders
- Credits to Stock
- 6 Minute Walk Test Recording Sheet - RT MMH514
- COPD Patient Knowledge Assessment MMH511
- Initial Respiratory Evaluation - MMH513
- Pulmonary Rehab Tracking Sheet MMH515

(Kerns/Brubaker) ***Approved (All)***

6.2 Organizational Chart Approval

The new Organizational Chart was approved. Brubaker asked why Louis Ward does not have a title. It should be listed at this time as "Director of Support Services" **(Hathaway/Whitney)** ***Approved All***

6.3 Election Resolutions for Modoc and Lassen County: Resolutions 2014-3/2014-4. **(Albaugh/Kerns)** ***Approved (All)***

7. INFORMATION/BOARD EDUCATION/ANNOUNCEMENTS

- Board Education – QHR Webinar 2nd Tuesday each month, 10 a.m. PST
- CCHAN Meeting July 10

8. ANNOUNCEMENT OF CLOSED SESSION: 2:52 pm

8.1 Government Code Section 54962

Quality Assurance: Quality Improvement Issues, Medical Staff Report (Dr. Dan Dahle, Chief of Staff)

Staff Status Change: (to inactive)

- ✓ Bradley Jones, MD
- ✓ Farzad Sabet, MD
- ✓ Laurie Watters, CRNA

Reappointment

- ✓ Maria Teresa Barton, CRNA
- ✓ Tom Watson, MD
- ✓ Todd Guthrie, MD

(Kerns/Hathaway) ***Approved (All)***

8.2 Government Code Section54957: Personnel – No action

8.3 Approve minutes of the July 30, 2014 Closed Session (Brubaker/Kerns) ***Approved (All)***

10. RECONVENE OPEN SESSION: 3:27 PM - REPORT ACTIONS TAKEN DURING CLOSED SESSION

11. ADJOURNMENT: There being no further business, at the hour of 3:53 p.m., President Albaugh declared the meeting adjourned. 3:28 pm

Attachment B

Mayers Memorial Hospital

Operations Report
July 2014

Statistics	July YTD FY15 *(current)*	July YTD FY14 *(prior)*	July Budget YTD FY15
Surgeries (*including C-sections)* ➢ Inpatient ➢ Outpatient			
Procedures *(surgery suite)*			
Inpatient (Acute/OB/Swing) Days	107	184	163
Emergency Room	372	413	400
Skilled Nursing Days	2266	2303	2182
OP Visits (OP/Lab/X-ray)	1473	1548	1358
Hospice Patient Days	118	200	60
PT	996	819	846
Ambulance Runs	38	29	34

Operations District-Wide

Matthew Rees, Chief Executive Officer

Administration/CEO activities during the past month:

- Dr. Syverson is now here and has been able to do some emergency surgeries as well as scheduled surgeries and procedures. The surgery staff is excited about being busy again. We also did our first knee replacement in years. We are tracking the financial impact and will be reporting regularly to the board.
- LTC survey took place and have turned in our plan of correction. Survey went well and no surprises in the written report.
- Fire Life Safety Survey took place and our panel for the fire system failed. We are on fire watch until we get it repaired or replaced.
- Evacuation of the Burney Facility during the local fires. I want to thank the staff for the great work that they did. All went well, both with the evacuation and the return of the patients. Everyone worked well as a team.
- Working with Boxer and LaMalfa's offices to get the state USDA RD office to move forward on our loan package. Boxer's office is contacting the state office and Lamalfa's office is contacting the federal office to get them inquiring about where the package is.
- Continuing to work with Mountain Valley's on integration of systems and recruitment of physicians.
- Preparing for the Intermountain Fair and working on promoting our facility to Canby and other areas.

Critical Access Hospital

Keith Earnest, Pharm.D., Chief Clinical Officer

I want to commend Sherry Wilson, and all the staff that helped with the evacuation. Mayers has the best staff and we all worked together to move our residents quickly and safely. Everyone had a willing attitude and helped out. It was a stressful time but we know we can handle these situations because we have the best people working for us.

Physical Therapy

- Our Physical Therapists are working with Modoc Medical Center to staff vacations of their PT department.
- We are promoting Mayers Physical Therapy services to orthopedic surgeons and the Canby Clinic.
- To make for smooth transitions of care, a Physical Therapist will meet and evaluate orthopedic surgery patients during their pre-op visit.

Laboratory

- A new registry CLS is scheduled to start in early September.
- The operations team is working with lab personnel to find ways to reduce late night call backs.

Imaging

- Our PACS is up and running. Staff is being trained and physicians will be trained shortly.
- Our vascular sonographer is relocating and Doreen Parker, Imaging Manager, is looking into having this role filled one day a week.

Pharmacy

- The new afterhours order processing company went live August 13th. All transitions can be bumpy but the new company is meeting our expectations.

Telemedicine

- Due to the low volume of referrals, the technician's hours have been reduced.

Hospice

Mary Ranquist, RN, is enthusiastically learning the computer program. She is getting her feet wet as manager. She is also the case manager for hospice. Gail Leonard, social working, is assisting with billing and claims denials. Michelle Peterson, RN, will be coordinating Hospice quality program.

Critical Access Hospital
Submitted by: Sherry Wilson CNO/Acute

~~~~~~

Infection Control

- Infection Control continues to work closely with CDPH and CDC with the Ebola virus crisis updates and mandates with reporting. Although this is not a major player in the intermountain area, it is required that we read updates and keep abreast of all activity occurring with this disease. Shasta County has had 1 death attributed to West Nile Virus, so precautions are being advised to use DEET, wear long sleeve shirts and pants if outdoors, and limit outdoor activities in dusk and dawn when the mosquitoes are most active.

Skilled Nursing Facility – Burney & FRM
Submitted By: Sherry Wilson, RN, CNO

- Census is at 74
- Just wanted to take this opportunity to express what an amazing job our staff did on the evacuation of the annex. The Team work was amazing to see and be part of. I cannot say Thank You enough to the many departments that offered their assistance to us that night and followed our residents down to Mercy Medical Center remaining by our residents until they were placed with accepting facilities. They AMAZED me with their compassion and dedication to our residents and our Organization. The Board should be very proud of our staff and the opportunity to work with such an amazing Team.
- With all the residents back safely we have began to take in new admits and are back to business as usual. We have three newly hired CNAS that are currently beginning the orientation process.

~~~~~~

ATTACHMENT C

SECTION 5. PRIVACY & SECURITY

Overview

The Privacy & Security section discusses the definition of personally identifiable information (PII) and protected health information (PHI), the Health Insurance Portability and Accountability Act (HIPAA) and when this confidential information can be used and disclosed. This section also discusses ways to keep information secure, how to report privacy and security violations and the rights individuals have regarding their personal information.

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) is any information that identifies or describes an individual. Some examples of information that can be PII include:

- Full Name
- Birthplace
- Email Address
- Vehicle registration plate number
- Credit card numbers
- Country, state, zip code or city of residence
- Name of school attended or workplace
- Social Security Number (SSN)
- Biometric records
- National Identification number
- Driver's license number
- Age
- Grades, salary or job position
- Date of birth
- Mother's maiden name

What is Protected Health Information (PHI)?

Information is considered PHI if it is individually identifiable and:

- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care;
- Was created/received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse (e.g. a 3rd party medical biller);

- Includes documents in ANY medium: written, oral, or electronic.

Examples of PHI include:

- Information doctors, nurses and other healthcare professionals put in a patient's medical record;
- Conversations a doctor has with nurses and other medical personnel about a patient's care or treatment;
- Information about an individual that resides in their doctor's and hospital's computer system;
- Billing information about a patient.

Patients' Privacy Rights

Mayers Memorial Hospital District has adopted procedures to give patients the following rights:

- Right to obtain a written notice from Mayers Memorial Hospital District explaining how it will use and disclose their information (the Notice of Privacy Practices).
- Right to access their medical records. This means patients can see their records, request copies, and request an amendment to the records. Limited exceptions to this right exist. (However, patients are not entitled to take the original record.)
- Right to request that certain information be restricted from use or disclosure for purposes of treatment, payment and health care operations (although Mayers Memorial Hospital District is not required to comply with such requests, except in limited circumstances).
- Right to obtain an accounting of how their information has been disclosed for purposes not related to treatment, payment or health care operations.
- Right to request that information be communicated to them in particular ways to ensure confidentiality, for example at work rather than at home.
- Right to refuse to authorize the release of information for most purposes not related to treatment, payment or health care operations.
- Right to be notified of breaches to the extent required by law.

In general, patients' privacy rights and the health information laws ensure that health information is used for health care-related purposes only.

All requests to exercise rights can be made by submitting a written request on the appropriate form. The forms are available in the Medical Records and/or Patient Access departments. Requests can also be made by the individual's personal representative, by filling out a form for use by such representatives.

Mayers Memorial Hospital District has also implemented safeguards to protect the PII it collects and uses in performing its functions. These safeguards are described in a later portion of this section.

What are the Privacy & Security Rules?

PHI is protected under federal regulations known as the Privacy Rule and the Security Rule. These regulations were developed as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and require privacy and security protections for individually identifiable health information. These HIPAA regulations are enforced by the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR).

The Privacy Rule covers ALL PHI, whether written, oral or electronic and includes:

- The use and disclosure of a patient's individually identifiable health information by organizations subject to the Privacy Rule (known as "covered entities").
- The ability for patients to understand and have more control over their health information and how it is used.

The Security Rule protects a patient's electronic protected health information, or e-PHI. A major goal of the Security Rule is to allow covered entities to use new, more efficient technologies to help improve the quality of patient care and still protect the privacy of a patient's health information.

Who Must Follow the Privacy & Security Rules?

Covered Entities

The entities that must follow HIPAA regulations are called "covered entities." Covered entities include health care providers, health plans and health care clearinghouses.

- **Health care providers** include any person or organization that provides, bills, or is paid for health care in the normal course of business, such as hospitals, doctors, nursing homes, clinics and pharmacies; these providers are covered entities if they transmit health information in electronic form to conduct transactions that are covered by HIPAA, such as electronically billing a health insurance company;
- **Health plans** include health insurance companies that provide or pay for the cost of medical care through a health plan, such as HMOs, company health plans and government health programs that pay for health care such as Medicare, Medi-Cal and military and veterans' health care programs.
- **Health care clearinghouses** are entities such as billing services, re-pricing companies, and community health management information systems that put nonstandard health information into a standard format or data content.

Business Associates

A "business associate" performs work for a covered entity that involves using or disclosing the covered entity's PHI. A business associate may be a contractor, subcontractor or vendor working for the covered entity, and can itself be a covered entity. Under HIPAA rules, the covered entity using the services of a business associate must have a written agreement with the business associate that requires the business associate to follow HIPAA privacy and security rules when it performs work involving the covered entity's PHI. The business associate can only use the PHI for the purpose for which the covered entity shares it.

Examples of business associates include: an independent medical transcriptionist that provides transcription service to a hospital; a third-party administrator that assists a health insurance company with claims processing; and a CPA firm whose accounting services involve access to PHI.

When Can PHI be Used and Disclosed?

Permitted Uses and Disclosures

A covered entity is permitted (but not required) to use and disclose PHI without a patient's authorization in the following situations:

- To the patient who is the subject of the PHI;
- For treatment, payment and health care operations activities:
    - "**Treatment**" means providing, coordinating or managing a patient's care, including consultations between providers and referrals.
    - "**Payment**" is defined as activities related to paying or being paid for services rendered. These include eligibility and coverage determinations, billing, claims management, utilization review and the like.
    - "**Health care operations**" covers a broad range of activities such as quality assessment and improvement, patient education and training, health practitioner training, contracting for health care services, medical review, legal services, auditing functions, business planning and development, business management and general administrative activities.
- Incident to an otherwise permitted use and disclosure. In this case, the PHI disclosed is related to PHI that has already been given permission to be used and disclosed.
- Public interest and benefit situations, for example, for law enforcement purposes, domestic violence reporting, and public health activities that involve safety or communicable disease.

Required Uses and Disclosures

A covered entity is *required* to disclose PHI in only 2 (two) situations:

- To patients when they request access to, or an accounting of disclosures of, their PHI. Limited exceptions to this requirement exist.
- To HHS when it is investigating the covered entity or determining its compliance with HIPAA.

Authorized Uses and Disclosures

A covered entity must obtain the patient's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.

Examples of disclosures that would require a patient's written authorization include: disclosures to a life insurer for coverage purposes; disclosures to an employer of the results of a pre-employment physical or lab test; and disclosures to a pharmaceutical firm for their own marketing purposes.

The Principle of "Minimum Necessary"

A central aspect of the Privacy Rule is the concept of "minimum necessary" use and disclosure. HIPAA requires that when using or disclosing PHI, or when requesting PHI from another covered entity or business associate, a covered entity must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

The minimum necessary requirements **do not** apply to the following:

- Disclosures to or requests by a doctor or hospital for treatment purposes;
- Disclosures to the patient who is the subject of the information;
- Uses or disclosures with a patient's authorization;
- Uses or disclosures required for HIPAA standard transactions;
- Disclosures to HHS when the disclosure of information is required under the Privacy Rule for enforcement purposes;
- Uses or disclosures required by law.

Safeguards and the Privacy Rule

The HIPAA Privacy Rule contains a broad security requirement that applies to all individually-identifiable health information in the hands of covered entities. The rule requires covered entities to have in place appropriate administrative, physical, and technical safeguards (described in further detail below) to protect the privacy of PHI. Mayers Memorial Hospital District has implemented reasonable safeguards that protect PHI from any intentional or unintentional use or disclosure that is in violation of HIPAA standards, and from incidental uses or disclosures.

This broad mandate applies to PHI in all forms – paper, oral and electronic. The requirement for administrative, physical, and technical safeguards tracks the broad categories of standards in the HIPAA Security Rule. While the standards of the Security Rule apply only to electronic PHI, many of the administrative and physical standards in the Security Rule have been expanded to include the security of paper and oral PHI.

Safeguards and the Security Rule

As with the Privacy Rule, the Security Rule also requires adherence to appropriate administrative, technical and physical safeguards. The Security Rule is narrower than the Privacy Rule because it protects only electronic PHI – that is, individually-identified health information that is transmitted by, or maintained in, electronic media. Following is a detailed description of administrative, technical and physical safeguards:

- **Administrative Safeguards.** The administrative safeguards provide a framework or foundation for the implementation and management of the other standards. They are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of Mayers Memorial Hospital District's workforce in relation to the protection of that information.
- **Physical Safeguards.** Physical protections are the first line of defense against intrusion. They are measures, policies and procedures to protection information and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.
- **Technical Safeguards.** Technical safeguards are at the heart of electronic health information security. The technical standards assume that someone has physical access to systems containing PHI, either onsite or remotely, and aim to erect technical barriers to unauthorized access to, or use of, the information. They consist of technology and related policies and procedures that protect e-PHI and control access to it.

Keeping Your Passwords Safe

One of the best ways to keep information secure is to create strong passwords. Some examples of guidelines to create strong passwords include:

- The best passwords use a combination of numbers, upper and lowercase letters and special characters such as: * & @ $
- Passwords should be at least 8 characters long
- If possible, do not use only letters or only numbers
- Do not use names of family members
- Do not leave the password blank
- A good password is easy to remember but hard to guess
- Consider using the first letter of the words in a phrase or song
    - Example: "To be or not to be" would equal "2bon2b"

It is not only important to create strong passwords; you must also practice behaviors that will keep your password safe. Some of these behaviors include:

- Do not write down your password
- Do not share your password with others
- Do not reuse passwords
- Change password every 30 to 60 days
- Avoid reusing the same password for at least a year

Protecting Your Workstation and Laptop

Protecting your workstation

Securing information when you leave your PC / Workstation is critical to maintaining information security. Here are some practices that will help safeguard information while stepping away from your desk:

- Always log off of desktops, laptops and any portable electronic devices that have network access, such as a smart phone.
- Ensure paper documents are secure at all times. Lock your workstation when not in use.
- Make sure your workstation screen is not visible to the public.
- Use only computers, networks, applications and information for which you are authorized.

Mayers Memorial Hospital District reserves the right to limit, restrict or extend access to its computer network and to its data resources.

Another aspect of information security to be mindful of is the potential of outside intruders entering the hospital. Some common intrusion tactics to be aware of:

- Unauthorized physical access

- Impersonation on calls to the hospital
- Wandering through halls looking for open offices
- Stealing sensitive documents

Protecting your laptop

Laptops often contain sensitive information. You are responsible for the confidentiality and security of your laptop. If your laptop is lost or stolen and contains sensitive information, you must report it to your supervisor and the HIPAA Compliance Officer. There are many ways in which you can better protect your laptop:

- Keep information secure on your laptop
- Data Encryption
- Virus Protection

Security While Traveling and Working Remotely

While laptops give us great freedom, they also come with special security issues. Here is a list of safeguards to help increase security while traveling and working remotely:

- Avoid using computer bags
- Use strong passwords, and do not keep them in your laptop bag
- Encrypt your data
- Carry your laptop with you
- Keep an eye on your laptop
- Avoid setting your laptop on the floor
- Try not to leave your laptop in your hotel room
- Use a laptop security cable
- Affix your name and contact info to your laptop
- Turn off your laptop's Wi-Fi capability when you are not using it
- Use a Virtual Private Network (VPN)
- Disable file and printer sharing
- Make your folders private
- Use a personal firewall
- Consider removing sensitive data from your laptop
- Use anti-virus software and keep it updated

E-Mail Security

When using e-mail, slow down, think and check before hitting send. Common mistakes include:

- Auto-complete: Microsoft Outlook completes addresses before your finish typing. Always verify the name and the e-mail address before you hit send.
- Copying and blind copying (cc/bcc): Take a look at who is on the "cc" list and "bcc" list. If your reply is sensitive in nature, you may want to reply only to the sender.

In order to ensure the security of the emails you send and receive, and to protect the information you are authorized to access, use and disclose, keep in mind the following do's and do not's of e-mail security of knowledge:

- Do's
    - Open e-mails only from people you know and trust;
    - Open only those e-mail attachments whose headings or texts sound familiar;
    - Use e-mail encryption for messages containing PHI or particularly sensitive information;
    - Delete suspicious messages;
- Do Not's
    - Do not provide your e-mail or someone else's e-mail address online;
    - Do not trust a site just because it claims to be secure;
    - Do not open e-mail attachments from unfamiliar sources;
    - Do not open e-mail attachments containing the following file extensions: .exe, .bat, .reg, .scr, .dll, or.pif;
    - Do not provide personal information, unless you are certain of a person or organization's authority to ask for it;
    - Do not respond to e-mails that request your personal or financial information.

Penalties for Violations of Privacy Laws

HIPAA Penalties

Under HIPAA, civil money penalties may be imposed upon both covered entities and business associates for violations of the HIPAA rules. The penalties are progressive and a minimum penalty may be imposed even if the covered entity did not know of the violation:

- For violations where the covered entity did not know and, by exercising reasonable diligence, would not have known, of the violation:
    - Minimum penalty of $100 per violation
    - Maximum penalty of $50,000 per violation
- For violations due to reasonable cause and not willful neglect:

    - Minimum penalty of $1,000 per violation
    - Maximum penalty of $50,000 per violation
- For violations due to willful neglect, but the violation is corrected within 30 days after the covered entity knew or should have known of the violation:
    - Minimum penalty of $10,000 per violation
    - Maximum penalty of $50,000 per violation
- For violations due to willful neglect and not corrected:
    - Penalty of $50,000 per violation
- For each tier of penalties, there is a maximum of $1.5 million that may be imposed for identical violations within a calendar year.

There are also criminal sanctions under HIPAA that can be imposed on covered entities:

- For knowingly obtaining or disclosing PHI in violation of the HIPAA rules, the penalties include a fine up to $50,000 and imprisonment up to one year;
- If the offense is committed under false pretenses, the penalties include a fine up to $100,000 and imprisonment up to five years;
- If the offense is committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the penalties include a fine up to $250,000 and imprisonment up to 10 years

California Penal Code Penalties
The California Penal Code makes it a crime to:

- Knowingly access and without permission alter, damage, delete, destroy or otherwise use any data, computer, computer system, or computer network to commit fraud or to wrongfully control or obtain money, property or data;
- Knowingly access and without permission take, copy or make use of any data from a computer, computer system, or computer network, or take or copy any supporting documentation;
- Knowingly access and without permission add, alter, damage, delete or destroy any data, computer, software or computer programs;
- Knowingly and without permission disrupt or cause the disruption of computer services or deny or cause the denial of computer services to an authorized user of a computer, computer system or computer network.

These offenses are punishable by a fine up to $10,000, imprisonment up to 3 (three) years or both fine and imprisonment. (Calif. Penal C., § 502(c)(1), (2), (4) and (5), and (d).) The Penal code also defines lesser offenses that are punishable by fine and imprisonment in county jail.

Employees
Any employee of Mayers Memorial Hospital District who violates privacy or security policies or procedures shall be subject to discipline, including termination of employment.

Duty to Detect and Report Incidents

All Mayers Memorial Hospital District staff and all contractors and vendors who have access to hospital data systems, services or networks, or access to any confidential information (PII, PHI) that is collected, maintained, used or disclosed by Mayers Memorial Hospital District, must immediately report any incident that may affect the confidentiality, security or integrity of the data or the systems.

This includes suspected incidents. You should not wait to confirm the incident happened, or to investigate what happened, but must immediately report any suspected incident.

When you report an incident, the Privacy or Security Officer can then take immediate actions to prevent harm and will direct you on what actions you need to take.

The duty to report includes both security incidents and privacy incidents.

Security Incidents

A Security Incident is defined as:

> Any real or potential attempt (successful or unsuccessful) to access and/or adversely affect Mayers Memorial Hospital District data, systems, services or networks, including online data, systems, services and networks, and including but not limited to any effect on data availability, loss of data, disclosure of proprietary information, illegal access and misuse or escalation of authorized access.

Examples of security incidents include, but are not limited to:

- **Unauthorized Access** – a person gains logical or physical access without permission to a network, system, application, data, or other IT resource;
- **Inappropriate Usage** – a person violates acceptable use of any network or computer policies;
- **Lost or Stolen Asset** – a Mayers Memorial Hospital District asset is lost or stolen or personal belongings of a Mayers Memorial Hospital District employee or contractor are stolen at a work location;
- **Malicious Code** – a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host;

Privacy Incidents

A Privacy Incident is defined as:

> The attempted or successful unauthorized access, use, disclosure, modification or destruction of Personally Identifiable Information (PII) or Protected Health Information (PHI) or interference with system operations in an information system that processes, maintains or stores PII or PHI.

Examples of privacy incidents include, but are not limited to:

- **Fax** – papers with PII are sent to the wrong fax number;

- **Mail** – a package containing papers with PII and PHI is mailed using standard U.S. postal service methods, but it arrives damaged and some papers may be missing or may have been seen by unauthorized persons;
- **Oral** – two employees discuss confidential application information in a lobby area, where other people walk through and can overhear them;
- **Unauthorized Access** – a computer file with personal information on patients, including income information, is sent to the wrong vendor who uploads it to the vendor's computer system and the file is accessed by the vendor's employees;
- **Unauthorized Use and Access** – an employee wants to work at home to catch up on a backlog so he/she sends files with patients' personal information to his/her home computer, where a visiting nephew views the file when the employee opens it;
- Minimum Necessary Violation – an employee schedules a patient for an upcoming visit and while in the application reviews the patient's test results on a previous encounter.

Reporting Security and Privacy Incidents

You must IMMEDIATELY REPORT a suspected or actual security or privacy incident to:

- Your supervisor and/or the Privacy and Security Officer
- Email: hipaa@mayersmemorial.com
- Telephone: (530) 336-5511 ext. 1154

The Privacy and/or Security Officer monitors the email and telephone number daily and will respond to all reports of incidents. They will contact you and provide you an Incident Report Form to fill out, which will ask for basic information about the incident. Either the Security Officer or the Privacy Officer will direct you on the next steps to be taken.

Investigating Security and Privacy Incidents

Based upon the information they receive, the Security and Privacy Officers will direct an investigation, determine what immediate action is needed, and develop a plan to identify gaps and to take corrective actions to prevent a future reoccurrence of a similar incident.

Prompt action may mitigate harm by stopping continued inappropriate access to PII or PHI. For example, if personal information has been publicly posted, it can be removed and the persons whose information was exposed can be notified so that they can take steps to protect themselves.

Your diligence in immediately reporting any suspected or actual incident is essential to keep Mayers Memorial Hospital District's confidential information and its data systems, services and networks safe and protected. With your help, Mayers Memorial Hospital District can keep its confidential information and systems secure