Attachment A

Chief Executive Officer
Louis Ward, MHA

Mayers Memorial Hospital District

Board of Directors
Regular Meeting
Minutes

January 30, 2019 – 1:00 pm
Boardroom (Fall River Mills)

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:** Beatriz Vasquez called the regular meeting to order at 1:01 pm on the above date.

BOARD MEMBERS PRESENT:	**STAFF PRESENT:**
Beatriz Vasquez, President	Louis Ward, CEO
Abe Hathaway, Vice President	Travis Lakey, CFO
Laura Beyer, Secretary	Ryan Harris, COO
Allen Albaugh, Treasurer	Keith Earnest, CCO
Jeanne Utterback	Candy Vculek, CNO
	Diana Groendyke
ABSENT:	Val Lakey, Board Clerk

2	**CALL FOR REQUEST FROM THE AUDIENCE - PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS**		
	None		
3	**APPROVAL OF MINUTES**		
	3.1 A motion/second carried; Board of Directors accepted the minutes of December 5, 2018.	***Beyer/Hathaway***	***Approved All***
4	**DEPARTMENT/OPERATIONS REPORTS/RECOGNITIONS**		
	4.1 A motion/second carried; Steve Holt was recognized as December Employee of the Month. Resolution 2019-2	***Albaugh/Hathaway***	***Approved All***
	4.2 **Director of Human Resources/Worker's Comp Report** – Candy Vculek reported for Libby (Family Emergency absence) Albaugh mentioned amount being spent on the recruiters. For the international search, we do not pay until we have actual recruits. Not a lot of results from Hunter Ambrose. This will be reassessed after evaluating the bonus incentives. We are still doing CNA program, just hired 5 from the previous class. Albaugh had questions with the housing. Libby helps to manage the process.		
	4.3 **Director of Nursing** – SNF – Diana Groendyke – Minor deficiencies are addressed and readdressed each month. Falls, med errors, etc., are tracked each month including a root cause analysis. Census is at 76 today. Viral outbreak at Burney just ended on the Jan 28. Will now be able to admit. Three female beds at FRM and Burney; 2 male at FRM. Working together with Acute for admissions. Working on filling the rest of the beds. Have been talking with neighboring facilities. Eastern Plumas will be coming to visit. There are 22 beds in memory care. CIT Training was beneficial for SNF staff. Hathaway noted that he visited the facility and was impressed with the cleanliness and overall condition of the residents and facility.		

5 BOARD COMMITTEES

5.1	**Finance Committee**			
	5.1.1	Committee Meeting Report: Need to change the signature card. Abe Hathaway and Allen Albaugh will be the signers on the account and the bank will take care of the stamp.		
	5.1.2	**November/December 2018** Financial Review, AP, AR and acceptance of financials.	***Utterback/ Beyer***	***Approved All***
	5.1.3	**Mindray Approval** – Purchase of equipment for the ER (already approved $113,000) Packet is for the upgrade of the acute system which was purchased in 2011 and is an Integrated system. Currently, we rely on ER staff for help. If the systems are integrated the information sharing for care between departments will be more efficient. Without the system upgrade we will have to determine how to coordinate. As far as finance, the vendor gave a GPO level 2 discount. Cost for upgrade will be more at a later date when it is not integrated at the same time as the ER installation. Finance committee is concerned about spending with cost of expansion. Lakey noted that we have about 80 days of cash coming. We have contingency in the project. CFO feels comfortable with our cash position. Albaugh is concerned about spending money until our new building is closer to completion. Utterback asked about Quality of care. Patient Care impact will not happen until ER system is in place. Hathaway moved to postpone until June 2019 meeting Albaugh second	***Hathaway/ Albaugh***	***Approved All***
	5.1.4	**Resolution 2019-01 Signing Authority** COO needs to be able to sign at the county for permits, etc.	***Albaugh/Beyer***	***Approved***
5.2	**Strategic Planning Committee**			
	5.2.1	**Committee Meeting Report** – Albaugh reported on the SP Committee meeting. Discussed the Burney Clinic concept. Harris will go to the county Jan 31.		
	5.2.2	**Burney Clinic -** Approval to move forward on the Burney Clinic. After we get the plans from the county the next step will be to get the architect to draw up plans ($155/hr). Staff will bring the board a general cost for the board to make a decision to move forward. Will be an action item on the Feb agenda.		
5.3	**Quality Committee**			
	5.3.1	Committee Meeting Report – Beyer reported on the Quality committee meeting. Template is complete for Quality reporting.		

5.3.2	Policies & Procedures for Approval – Six Minute Walk Distance Test 2. Discharge Six Minute Walk Distance Test MMH620 3. Initial Six Minute Walk Distance Test MMH619 4. Breach Notification 5. Care of Dietary and Nutritional Services for Swing Bed Patients 6. Charging for Copies of PHI 7. Communication of PHI 8. Confidential Communications 9. Conflicts of Interest 10. Core Privileges, General Surgery 11. Exercise Prescription - Pulmonary Rehab MMH638 12. Exercise Tracking Sheet - Pulmonary Rehab MMH639 13. Fundraising and PHI 14. Guest Trays 15. HIPAA Privacy Officer and Privacy Program 16. Identity Verification 17. Individual Treatment Plan MMH628 18. Initial Interview Form Pulmonary Rehab MMH627 19. Non-Retaliation 20. Notice of Privacy Practices Policy 21. Nutritional Assessment - Pulmonary Rehab MMH632 22. Patient Quiz - Pulmonary Rehab MMH631 23. Pulmonary Rehab Patient Consent MMH637 24. Pulmonary Rehab Skills and Competency Assessment MMH636 25. Pulmonary Rehab Weekly Schedule MMH640 26. Pulmonary Rehabilitation Program 27. Reporting Compliance and Ethics Concerns 28. Senior Fitness Testing Personal Profile Form MMH622 29. Senior Fitness Testing, Pulmonary Rehab 30. Telemed Referral Form, MVHC MMH645 31. UCD Pediatrics Critical Care Cart - Telemedicine 32. Use and Disclosure for Workers Compensation 33. Workplace Violence Prevention Policy	***Utterback/Albaugh***	***Approval All***
6	**NEW BUSINESS**		
6.1	**Approval of Organizational Chart**	***Albaugh/Utterback***	***Approved All***
6.2	**Approval of Revised 2019 Calendar**	***Vasquez/Beyer***	***Approved All***
6.3	**February Meeting Date:** Monday, February 25, 2019	***Utterback/Beyer***	***Approved All***
7	**ADMINISTRATIVE REPORTS**		
7.1	**Chief's Reports**		

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.

7.1.1 **CEO:** Highlighted staffing. There will be a staffing committee set-up. Strategic goal meetings. Conversations with REMSA. SEMSA is trying to renegotiate contract with Air Methods. Helicopter will be day based at MMHD for now (pending approval). SEMSA is meeting on February 4 to see if that can be done. There are a lot of conversations that need to happen. SEMSA used the 180 day "Out clause" to terminate the contract. It will end on June 25. There will be the potential for an amendment depending on how the conversations go. There will be an Ad Hoc meeting in Big Valley on January 31; looking at options for Big Valley. Looking for a sustainable long-term solution.

Awaiting license for retail pharmacy.
Discussed transition team for new building.
Tour of laundry facility next month.
CEO meeting in Quincy (Staffing, building); will meet quarterly.
Went to Enloe to look at signage, etc.
Introduced Hailey Myers – Job Shadowing Student.
See written report.

7.1.2 **CCO**: Nurse Educator and Respiratory Therapist will be at FRHS January 31 discussing the dangers of vaping.

Albaugh asked about Occupational Therapy (OT) – there are things that need to be done for the license in order to make that happen.

7.1.3 **CFO**: Spent about $252,000 while government was shutdown. We will be reimbursed. We should be at about 140-150 days cash on hand by the end of the fiscal year.

7.1.4 **CNO**: Reviewed staffing for nursing. We have about 34 vacancies in the nursing staff. Ratios were discussed. (See excel spreadsheet)

Relias learning management system has been put in place.

Stroke protocol in ER – we now have an agreement with UC Davis - will also apply to neuro consults – should go in place on Feb 15.

7.1.5 **COO**: We had Fire, Life, Safety this week. It went well; we received a few minor deficiencies. Surveyor gave us a compliment.

Riverview House renovation has begun.

Building - Concrete pour was Jan 29; important milestone. Will able to start exterior wall framing. Keeping it to a 40-degree temperature for one week. IOR is OSHPD liaison. Current model reflecting a Sep 5, 2019 completion date.

Extension filed on 2020 deadline to demolish old building.

Worked through work required – skilled and trained work force.

7.2 **Construction Change Orders**: None

8 **OTHER INFORMATION/ANNOUNCEMENTS**

8.1 **Form 700 Reminder**
Vasquez and Utterback attended the ACHD Leadership Conference. Utterback commented on the event.

9	**ANNOUNCEMENT OF CLOSED SESSION** – 3:22			
	9.1	Government Section Code 54962 • Quality Assurance: Quality Improvement Issues, Medical Staff Report MEDICAL STAFF REAPPOINTMENT 1. Chuck Colas, DO – Emergency Medicine 2. Paul Davainis, MD – Emergency Medicine 3. Jeremy Austin, MD – Emergency Care 4. David Panossian, MD – Pulmonary Care 5. Julia Mooney, MD – Pathology MEDICAL STAFF APPOINTMENT 1. Steven McKenzie, MD – Consulting Family Medicine 2. Javeed Siddiqui, MD – Telemed. Infectious Diseases 3. Eric Stirling, MD – Consulting Emergency Medicine ADDITIONAL PRIVILEGES 1. Dale Syverson, MD – Anesthesia Privileges	***Utterback/Beyer***	***Approved All***
	9.2	**Real Property Government Code 54956.8 –** Closed on purchase of Pharmacy Building on Dec 21, 2018		
	9.3	**Litigation Government Code 54956.9** No Action		
	9.4	**Personnel Government Code 54957** ***Approve CEO goals***	***Utterback/Beyer***	***Approved All***
10	**RECONVENE OPEN SESSION: 4:25pm**			
11	**ADJOURNMENT**			

Next Regular Meeting – February 25, 2019 – Burney

I, _____, Board of Directors _____, certify that the above is a true and correct transcript from the minutes of the regular meeting of the Board of Directors of Mayers Memorial Hospital District

_____ Board Member

_____ Board Clerk

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.

Mayers Memorial Hospital District
Always Caring. Always Here.

RESOLUTION NO. 2019-03

A RESOLUTION OF THE BOARD OF TRUSTEES OF MAYERS MEMORIAL HOSPITAL DISTRICT RECOGNIZING

Nichole Strahorn

As January 2019 EMPLOYEE OF THE MONTH

WHEREAS, the Board of Trustees has adopted the MMHD Employee Recognition Program to identify exceptional employees who deserve to be recognized and honored for their contribution to MMHD; and

WHEREAS, such recognition is given to the employee meeting the criteria of the program, namely exceptional customer service, professionalism, high ethical standards, initiative, innovation, teamwork, productivity, and service as a role model for other employees; and

WHEREAS, the MMHD Employee Recognition Committee has considered all nominations for the MMHD Employee Recognition Program;

NOW, THEREFORE, BE IT RESOLVED that, Nichole Strahorn is hereby named Mayers Memorial Hospital District Employee of the Month for January 2019; and

DULY PASSED AND ADOPTED this 25th day of February 2019 by the Board of Trustees of Mayers Memorial Hospital District by the following vote:

AYES:
NOES:
ABSENT:
ABSTAIN:

_____
Beatriz Vasquez, CHAIRMAN
Board of Trustees, Mayers Memorial Hospital District

ATTEST:

_____
Val Lakey
Clerk of the Board of Directors

Mayers Memorial Hospital District
Always Caring. Always Here.

Marketing and Public Relations – Valerie Lakey, Director of Public Relations Report – February 2019

Mayers Memorial Hospital District Public Relations Department is working on Consistency and a recognizable brand. The goal has been to utilize low-cost/ no-cost avenues for public relations and keep our image in the public eye. We have been focusing on our community image and developing relationships with the schools, community organizations and businesses.

Accomplishments:

- **Budget –** The budget remains consistent with previous years. We have eliminated the television advertising for the 2019 calendar year and will be using those budgeted resources in other areas. We have designated an amount for the IMAGE budget. We will look at some television opportunities once the new building is completed.

- **Website** – New additions – low cost method to present message. Required for transparency. We have also implemented an INTRANET for employee use. This has allowed easier communication with employees and provides them a "one stop shop" for things they regularly need.
- **Social media** - Having a presence on Social Media is very important, as much of our target market uses these avenues. ***NO COST – except time. Schedule Posts, etc.***

- **Community Outreach – IMAGE BUDGET** - We continue to advertising locally in an effort to reduce out-migration. Keeping MMHD "visible" in the community is a high priority. We participate in health fairs and other community events; like the Intermountain Fair, which is a highly populated event for the Intermountain Area. We remain active in the local high schools with Health Career Days and High School Senior Internships. ***"Planting Seeds and Growing Our Own"*** has been a focus. We are also active with activities in local elementary schools.

- **Statewide recognition** – We have receive Statewide Awards including the Hospital Council Innovative Challenge Award and BETA GEM of the Year Award for our outreach projects: your:life and Planting Seeds…Growing Our Own. This is positive PR and goes a long way to promote our IMAGE! We will be presenting our initiative at the WHA Conference in Colorado. Additionally, I will be speaking at Stanford in March about our your:life project at their international Wellness Summit.

- **Department Marketing/Employee Public Relations –** Continue to work with department managers to market departments to the clinics and community.

- **Annual Report –** negotiated savings (pre-pay to save 15%) we mailed 7000 copies in January.

- **New Facility** – we are planning for IMAGE and branding of new building.

Last Quality project reported:	**Current report date to Board**
First Responder Awareness (FRA) HazMat Training; Disaster Preparedness **Update on last Quality project reported:** Continued FRA training for Maintenance, Environmental Services and Chiefs Participated in the Statewide Drill Developed new Emergency Preparedness Training for staff	02/12/19 **Last report date to Board Quality:** 10/10/18

What successes have you seen based on the outcome of previous Quality projects?

Through the variety of EP trainings over the last 6 months, we have seen an increase in the interest from staff about being involved in EP. We are beginning to have specific department personnel expand knowledge and continue education. Additionally, we completed the Emergency Preparedness portion of the Fire, Life Safety survey and had minor corrections to be made. Education and training is seeing results.

What issues have come up in your department relating to Quality?

Lack of time and resources to get staff trained. These are important issues, as we are surveyed on EP now.

PLAN: What plan was implemented to address those issues?

We are working on a training plan to be implemented in orientation and re-orientation. We are identifying those that need specific training. We are making sure ALL management is trained and designates a member of their staff to serve on safety committee and be a part of furthering and developing our EP program

DO: How did the implementation of that plan go?

In progress

STUDY: What kind of results did the implementation of the plan yield?

So far the results have been positive, as noted by the successful survey. We trained over 100 staff in ICS100/200 and our EP Program.

ACT: What changes were made based on the results of the plan implementation?

None so far as we are still in the process.

Upcoming Quality Items:	Quality Related Goals for the Department:
Management EP training	Training of designated staff in each department

Data/Graphics supporting project outcomes:

Attachment D

Mayers Healthcare Foundation
Quarterly Report
February 2019

The ***Mayers Healthcare Foundation board met on January 21, 2019.*** Below is a brief outline of business:

- Scholarship Committee proposed changes to program. Some changes have been implemented; others to occur throughout the year. A new application format has been developed for two separate scholarship categories: 1) community (i.e., high school seniors, college students); and, 2) Mayers employees.

- Financial Reporting: P&L January – December 2018; Balance Sheet (current), Contributions Summary Report Nov 1-Dec 31, 2018 including 52 donors and fund designations.

- Campaign Report: Over $3.1 million has been raised with less than $200K in receivables Foundation side/$1 million in receivables Hospital side. The McConnell Foundation will award the $1 million to the District in June. The foundation finance committee met with Travis Lakey, CFO, to determine the process for disbursing campaign funds to the District. The California Endowment $100K grant for NHW equipment will be awarded to the District this month—with payments to the District to follow in March 2019.

- 2018 Grant PowerPoint presentation by Sheba Sawyer. Grant funds for 2018 totaled $64,000 and although we had a few challenges in ’18 I am pleased to report Sheba Sawyer has done a lot of good background work and research going forward. We met to strategize for 2019 goals leveraging the new relationships from ’18 into concrete funding opportunities to increase funding. We have budgeted $100K for CY19--$50K Foundation/$50K District. Louis Ward invited Sheba to a recent OMT meeting to present; she will also present to management at its April meeting. She is currently working on two grant proposals due in March.

- Fundraising! Fundraising! Fundraising!
  - Hospice Annual dinner will be held April 5, 2019 – details to follow.

  - Chocolate Festival held January 27th was a great success with over 40 chocolate dessert entries, raising $13,000 for advanced hospital security technology. Much appreciation and thanks to the bakers, Crumb’s for the soups, raffle prize donors, auctioneer Craig Harrington, Pine Grove 4H, FRHS Interact Club, IM Fair Court, auction buyers, event sponsors and last but not least a thank you to ALL the volunteers that make this event happen. Please note the following generous event sponsors:

    Nurse and Professional Healthcare
    Advantage Pharmaceuticals / Art and Caroline Whitney
    SEMSA
    Driscoll's Inc.
    Dignity Health
    Tri Counties Bank

Do It Best Valley Hardware & Nursery
Mountain Valleys Health Centers
Assemblyman Brian Dahle
K & K Distributing
Allscripts
Dr. Michael Maier, Chiropractor
Plumas Bank
Precision Lube

A special thank you to the district directors for your collective personal contribution for the raffle prize—the gift certificates for local dining was a great gift! Thanks for your support!

- The board approved $40,000 for this year's Award Cycle currently in process. The announcement has been made to the management team and applications are due March 29th. Monies for equipment will be awarded in May. The funding source is coming from the Lucky Finds Thrift Store revenues. If you have the opportunity, please thank the volunteers.

- The foundation P&P review process was conducted by the board with edits and changes to policies; approved for implementation.

- 38th Annual Community Health Fair will be held April 6th @ the IM Fairgrounds, Ingram Hall. Barbara Spalding, Events Director, is planning and organizing the event to be even bigger and better. Please join us at the health fair!

In closing, a few things I'm working on…1) wrapping up the 2018 Donor Recognition Power Point presentation for the front lobby to thank our many generous donors supporting Mayers Memorial Hospital; 2) continue to meet with prospect donors; 3) preparing for the 2018 taxes for CPA; and planning and organizing an upcoming strategic planning session. There is a lot going on in the fundraising world. Thanks for the opportunity to report our business and activities.

Regards,
Marlene McArthur

Assembly Bill No. 2190

CHAPTER 673

An act to add Sections 130062 and 130066 to the Health and Safety Code, relating to hospitals.

[Approved by Governor September 22, 2018. Filed with Secretary of State September 22, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2190, Reyes. Hospitals: seismic safety.

Existing law, the Alfred E. Alquist Hospital Facilities Seismic Safety Act of 1983, establishes, under the jurisdiction of the Office of Statewide Health Planning and Development, a program of seismic safety building standards for certain hospitals constructed on and after March 7, 1973. A violation of any provision of the act is a misdemeanor.

Existing law provides that, after January 1, 2008, a general acute care hospital building that is determined to be a potential risk of collapse or to pose significant loss of life in the event of seismic activity be used only for nonacute care hospital purposes, except that the office may grant 5-year and 2-year extensions under prescribed circumstances, except as specified. Existing law requires an owner of a general acute care hospital building that is classified as nonconforming to submit a report to the office no later than November 1, 2010, describing the status of each building in complying with the extension provisions, and to annually update the office with any changes or adjustments. Existing law authorizes certain hospital owners who do not have the financial capacity or other reasons to bring certain buildings into compliance by the January 1, 2013, deadline to instead replace those buildings or take other action by January 1, 2020, as specified.

This bill would require all hospitals with buildings subject to the January 1, 2020, deadline described above and that are seeking an extension for their buildings to submit an application to the Office of Statewide Health Planning and Development by April 1, 2019, that specifies the seismic compliance method each building will use, as specified. The bill would require the office to grant an additional extension of time to an owner who is subject to the January 1, 2020, deadline if specified conditions are met. The bill would authorize the additional extension to be until July 1, 2022, if the compliance plan is based upon replacement or retrofit, as defined, or up to 5 years if the compliance plan is for a rebuild, as defined. The bill would require the office, before June 1, 2019, to provide the Legislature with a specified inventory of the hospital buildings. The bill would authorize the office to promulgate emergency regulations as necessary to implement these provisions.

Existing law requires, no later than January 1, 2030, the owner of an acute care inpatient hospital to either demolish, replace, or change to nonacute care use a hospital building that is not in substantial compliance with certain seismic safety regulations and standards developed by the office, or to seismically retrofit the building so that it is in substantial compliance.

This bill would require, before January 1, 2020, the owner of an acute care inpatient hospital whose building does not substantially comply with the above-described seismic safety regulations or standards to submit to the office an attestation that the board of directors of that hospital is aware that the hospital building is required to meet the January 1, 2030, deadline for substantial compliance with those regulations and standards.

By imposing new requirements under the act for owners of hospitals with regard to extension applications and the above-described attestation, this bill would expand the scope of a crime, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

The people of the State of California do enact as follows:

SECTION 1. Section 130062 is added to the Health and Safety Code, to read:

130062. (a) For the purposes of this section, the following terms have the following meanings:

(1) "Rebuild plan" means a plan to meet seismic standards primarily by constructing a new conforming SPC-5 building for use in lieu of an SPC-1 building.

(2) "Removal plan" means a plan to meet seismic standards primarily by removing acute care services or beds from the hospital's license.

(3) "Replacement plan" means a plan to meet seismic standards primarily by relocating acute care services or beds from nonconforming buildings into a conforming building.

(4) "Retrofit plan" means a plan to meet seismic standards primarily by modifying the building in a manner that brings the building up to SPC-2, SPC-4D, or SPC-5 standards.

(b) All hospitals seeking an extension for their SPC-1 buildings shall submit to the office an application, in a manner acceptable to the office, by April 1, 2019. At a minimum, the application shall state which of the seismic compliance methods described in subdivision (a) will be used for each SPC-1 building.

(c) A hospital owner that has been granted an extension pursuant to subdivision (g) of Section 130060 or subdivision (b) of Section 130061.5

may request, and the office shall grant, an additional extension of time as set forth in this section.

(d) (1) For a hospital that seeks an extension for compliance based on a replacement plan or retrofit plan, the owner shall submit a construction schedule, obtain a building permit, and begin construction by April 1, 2020.

(2) Using the construction schedule submitted pursuant to paragraph (1), the hospital and the office shall identify at least two major milestones relating to the compliance plan that will be used as the basis for determining whether the hospital is making adequate progress toward meeting the seismic compliance deadline.

(3) Failure to comply with the requirements described in paragraph (1) or (2), or to meet any milestone agreed to pursuant to paragraph (2), shall result in the assessment of a fine of five thousand dollars ($5,000) per calendar day until the requirements or milestones, respectively, are met.

(4) Final seismic compliance shall be achieved by July 1, 2022.

(e) (1) For a hospital that seeks an extension for compliance based on a rebuild plan, the office shall grant an extension of up to five years. The owner shall submit, in a manner acceptable to the office, no later than July 1, 2020, the rebuild plan, deemed ready for review, and shall submit a construction schedule, obtain a building permit, and begin construction no later than January 1, 2022.

(2) The hospital and the office shall identify at least two major milestones, agreed upon by the hospital and the office, that will be used as the basis for determining whether the hospital is making adequate progress toward meeting the seismic compliance deadline.

(3) Failure to comply with the requirements described in paragraph (1) or (4), or to meet any milestone agreed to pursuant to paragraph (2) or (4), shall result in the assessment of a fine of five thousand dollars ($5,000) per calendar day until the requirements or milestones, respectively, are met.

(4) For a hospital that has previously submitted to the office a rebuild project under construction, the office may accept certification from the hospital that it has obtained appropriate building permits consistent with an approved incremental plan review and that construction thereunder has commenced and is continuing. The previously approved construction schedule shall be amended to reflect the extension being requested, and at least two new major milestones shall be identified. The owner shall not be required to resubmit construction plans previously submitted to the office, and the office may not impose new or different requirements for any increment already approved or building permit already issued by the office as a condition for granting an extension.

(5) Final seismic compliance shall be achieved, and a certificate of occupancy shall be obtained, by January 1, 2025.

(f) The office may grant an adjustment to the requirements described in paragraph (1) or (2) of subdivision (d) or paragraph (1) or (4) of subdivision (e), or the milestones agreed to pursuant to paragraph (2) of subdivision (d) or paragraph (2) or (4) of subdivision (e), as necessary to deal with contractor, labor, or material delays, or with acts of God, or with

governmental entitlements, experienced by the hospital. If that adjustment is granted, the hospital shall submit a revised construction schedule, and the hospital and the office shall identify at least two new major milestones consistent with the adjustment. Failure to comply with the revised construction schedule or meet any of the major milestones shall result in penalties as specified in paragraph (3) of subdivision (d) and paragraph (3) of subdivision (e). The adjustment shall not exceed the corresponding final seismic compliance date specified in paragraph (4) of subdivision (d) or paragraph (5) of subdivision (e).

(g) The duration of an extension granted by the office pursuant to this section shall not exceed the maximums permitted by this section. Moreover, within that limit, the office shall not grant an extension that exceeds the amount of time needed by the owner to come into compliance. The determination by the office regarding the length of the extension to be granted shall be based upon a showing by the owner of the facts necessitating the additional time. It shall include a review of the plan and all the documentation submitted in the application for the extension, and shall permit only that additional time necessary to allow the owner to deal with compliance plan issues that cannot be fully met without the extension.

(h) No extension shall be granted pursuant to this section for SPC-1 buildings unless the owner has submitted to the office, by January 1, 2018, a seismic compliance plan.

(i) An extension shall not be granted pursuant to this section for seismic compliance based upon a removal plan.

(j) In lieu of the reporting requirements described in Section 130061, a hospital granted an extension pursuant to this section shall provide a quarterly status report to the office, with the first report due on July 1, 2019, and every October 1, January 1, April 1, and July 1 thereafter, until seismic compliance is achieved. The office shall post the status reports on its Internet Web site.

(k) Before June 1, 2019, the office shall provide the Legislature with an inventory of the SPC category of each hospital building. A report submitted to the Legislature pursuant to this subdivision shall be submitted in compliance with Section 9795 of the Government Code.

(*l*) (1) The office may revoke an extension granted pursuant to this section for a hospital building where the assessment for a penalty exceeds 60 days.

(2) Notwithstanding any other law, any penalties assessed pursuant to this section shall be deposited into the General Fund within 45 days of assessment or within 45 days following a determination on appeal, if any. A hospital assessed a penalty pursuant to this section may appeal the assessment to the Hospital Building Safety Board, provided the hospital posts the funds for any penalties with the office, to be held pending the resolution of the appeal.

(3) The office shall not issue a construction final or certificate of occupancy for the building until all assessed penalties accrued pursuant to this section have been paid in full or, if an appeal is pending, have been posted subject to resolution of the appeal. Penalties deposited by the hospital

pursuant to paragraph (2) shall be considered paid in full for purposes of issuing a construction final or certificate of occupancy. This paragraph is in addition to, and is not intended to supersede, any other requirements that must be met by the hospital for issuance of a construction final or certificate of occupancy.

(m) The office may promulgate emergency regulations as necessary to implement this section.

SEC. 2. Section 130066 is added to the Health and Safety Code, to read:

130066. Before January 1, 2020, the owner of an acute care inpatient hospital whose building does not substantially comply with the seismic safety regulations or standards described in Section 130065 shall submit to the office an attestation that the board of directors of that hospital is aware that the hospital building is required to meet the January 1, 2030, deadline for substantial compliance with those regulations and standards.

SEC. 3. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

Attachment F

Operations Report
February 2019

Statistics	January YTD FY19 *(current)*	January YTD FY18 *(prior)*	January Budget YTD FY19
Surgeries (*including C-sections)*	35	96	96
➢Inpatient	1	15	24
➢Outpatient	34	81	72
Procedures *(surgery suite)*	73	150	192
Inpatient	1115	1291	1288
Emergency Room	2394	2442	2465
Skilled Nursing Days	15933	16180	15848
OP Visits (OP/Lab/X-ray)	8725	9858	9163
Hospice Patient Days	919	861	728
PT	1937	2307	1925

Operations District-Wide
Louis Ward, MHA, CEO

MMHD Ambulance Services

- Mayers Memorial Hospital District Administration and Staff have worked closely with our regional EMS partners and SEMSA leadership throughout the past month in an effort to preserve the established relationship MMHD has with SEMSA, the agency currently contracted to operate the MMHD ambulance service. At the time of this written report there are ongoing negotiations occurring which could result in SEMSA continuing to provide ground transport in the intermountain area. Negotiations are also occurring with Air Methods the parent company of the helicopter servicing the area. If these negotiations are successful both Air and Ground transport will be preserved in the intermountain area with little changes.

- As stated in past BOD meetings, as well as published in the Intermountain News and Mountain Echo; Mayers Memorial Hospital District will operate the ground ambulance service in the case negotiations with SEMSA are not successful. There will be no interruption in ambulance service in the intermountain area. Administration is working with nurse leadership to draft a request for proposal (RFP) document that will be published and distributed to EMS agencies with a proven history of collaborating with hospitals to operate ambulance services. If negotiations are not successful with SEMSA the RFP process will begin in March.

- More information will be provided verbally at the BOD meeting.

Transition Steering Committee

- The District is forming a "Transition Steering Committee" which will be tasked with planning and carrying out the move from the current space housing the Emergency Room, Lab, Imaging, Patient Access, Administration, and Business Office to the new wing expected to open in September of this

year. This committee will be chaired by J.D Phipps, Director of Emergency & Ancillary Services. The first meeting of this committee will occur in early March with subsequent meetings to occur frequently thereafter. The committee chair will be required to present progress to the Operations Team bi-weekly, this information will also be shared with the Board of Directors monthly by the COO and the CNO.

Management Orientation

- District Administration is working closely with the Operations Team and Human Resources to develop and implement a standardized approach to onboarding new managers. This new process, which we will call the district management orientation, will continue to take shape over the next few months as we are collaborating with all current managers in how the orientation should look and feel. The first step in the development of the management orientation will be setting a baseline of the current management team's understanding of the function of a manager and the tools currently provided to them. We will establish this baseline with a management quiz, which has been developed with the assistance of HR and the Operations Team. The management quiz will be distributed using a survey monkey, data will be collected, and trends will be discovered. Once the team has a better understanding of any current knowledge gaps we will develop a plan to mitigate current knowledge deficiencies and prevent them in the future by incorporating education into the management orientation. We look forward to working on this project and will report to BOD quality and the full BOD in future meetings.

CMS Meaningful Use Attestation 2018

- The District will once again attest to meeting the CMS Meaningful Use (MU) requirements in late February. The MU program requires hospital to continuously update their electronic medical record (EMR) systems as well as increase utilization of EMR systems each year. This is the Districts 5th year in a row meeting all of the necessary requirements set forth in the government quality and interoperability program.

Retail Pharmacy

- The District has made significant progress this past month in our efforts to bring a community pharmacy to the Fall River Valley. Staff has completed the licensure application and submitted it to the California State Board of Pharmacy. The Board of Pharmacy states it can take up to 6 weeks for the application to be accepted and a license to be granted; at this point, we are anticipating seeing this in March. Staff has also filed a Fictitious Business Name Statement with the County which is required as part of the Board of Pharmacy Application, we are also awaiting a response on this submittal. Once we receive licensure staff will then work with the Drug Enforcement Agency (DEA) to obtain a DEA #. Finally, we will then submit an application for a Medi-Cal provider number.

- In collaboration with our retail pharmacist and a consultant, staff has completed the design of the interior of the retail pharmacy. We are now preparing to work with our architect to develop a set of construction documents that will be used to obtain a permit from Shasta County, once we have the permit we will begin construction on the interior. Our anticipated opening date is May 15th. More information to be provided verbally at the BOD meeting.

Employee Meetings

- Administration is preparing materials for our upcoming quarterly employee meetings occurring on March 6th and 7th. As previously reported Administration strives to meet with employees at both facilities once a quarter in an effort to update the group on district activities and provide education when necessary. These meetings assist employees and management by increasing communication so we can deliver meaningful and prompt solutions to any issues the district and employees face. I look forward to these meetings as it is a great way for us all to engage in good dialogue, which has proven to be very successful in the past.

WHAAS 2019 Conference

- Valerie Lakey, Dir. Of Public Relations and I will attend the Western Healthcare Alliance Annual Summit (WHAAS) the last week of February. The Western Healthcare Alliance is an association of dozens of Critical Access Hospitals from California, Washington, and Colorado. We are excited and honored to also have been chosen as a featured presenter at the conference. We will be presenting to the group MMHD's Planting Seeds and Growing Our Own initiative. This program continues to be a program hospitals throughout CA and now the Western United States are interested in replicating. We are proud to have been chosen and look forward to showing off the good work the staff here at Mayers is doing. A huge thanks to Val Lakey for her passion and continued commitment to this amazing program.

Respectfully Submitted by,
Louis Ward, MHA
Chief Executive Officer

Chief Operating Officer Report

Prepared: Ryan Harris, COO

Hospital Expansion Project

- We had a successful concrete roof deck pour and were able to maintain temperatures in the building above the required 40 degrees. The metal stud contractor is continuing to work on both interior and exterior metal studs. Over the next two weeks you will start to see the exterior densglass sheathing be installed, work to continue on the lobby roof, and plumbing rough-in. As of February 19th I am awaiting an updated schedule from Layton Construction. If received before the February 25th board meeting I will present it to the board.

- MMHD has received and approved Layton Construction's skilled and trained workforce compliance plan, as well as the formal request to substitute the concrete contractor with one that can meet the requirement. This was sent to the labor commissioner with all documents and an approved payment was released to Layton Construction.

- Current scheduling models reflect a September completion.

Facilities, Engineering, Other Construction Projects

- MMHD Staff is still working through the design phase of the pharmacy project. My goal is to have a final conceptual design to show to the board at the February 25th board meeting.

- More will be reported at the board meeting in regards to the Burney Clinic space.

- Other projects I am working on with Greenbough Design are closing out the 2015 fire panel project with OSHPD, AC 9 emergency replacement project, Long Term HVAC replacement project, phase 3 of the SNF renovation, the demolition of the 1956 building, a facility-wide building inventory and use project and a new space within the hospital for a sonography/ultrasound room. A kickoff meeting will be held for the 1956 building demo project on 2/20/19. More to be reported at the board meeting.

- Some of the projects our Facilities and Engineering department are currently working on include finishing the Burney Annex Access Control project, finishing the Laundry Facility, installing a new center island at the Burney Annex, reconfiguring the maintenance shop, implementation of a stocking system through Grainger, and they have started the Riverview house remodel this month with an anticipated completion in June 2019.

- Some of the upcoming projects our Facilities and Engineering Department will be working on are finishing the last phase of the SNF renovation project, conversion of the MVHC clinic building into office space, and remodeling the current finance building into an administration building.

IT

- Current and upcoming IT department projects include: upgrading the network components throughout the facility, moving the telemedicine connection to the secure Telehealth network, setting up a bi-direction interface for Sac Valley Med Share Health Information Exchange (HIE), planning the implementation of a next-generation firewall, assist with Pacs replacement and migration, preparing for the networking and connection to the Fall River Campus onsite clinic space once MVHC moves, as well as the new pharmacy building.

Purchasing

- Steve Sweet, our IT department and I have started a new project to streamline our requisition process using either a web-based software or paragon. This is an ongoing project and more will be reported over the next several months.

- Our purchasing team is also working on the purchasing process for all the equipment going into the new building. Steve Sweet has been working with departmental staff to go over their equipment list and finalize the equipment needed in the expansion building.

Dietary

- Susan Garcia, the dietary staff, and I are working to finish up the PRIME project for reporting in March, looking into replacement menu systems that will work best for the dietary department and our residents, looking into ways to improve communication within our department and team,

revising departmental work tasks and responsibilities and updating our new orientation procedures. One new twist to the PRIME project was the need to remove soda sales from both facilities in order to meet the requirements of the project.

- We will also be implementing a new point of sale system which will be put in place by the end of the fiscal year.

Security

- I have no security incidents to report.

Environmental Services & Laundry

- Our go live date for Laundry is still set for March 7, 2019. We will start the phasing out of our Aramark linens on Monday February 25th at the Burney Annex and in Fall River the following Monday. Staff is ready to start this transition as we have been preparing for this for the last year.

Chief Nursing Officer Report

Prepared by: Candy Vculek, CNO

- No written report.

Chief Clinical Officer Report

Prepared by: Keith Earnest, Pharm.D., CCO

Pharmacy

- No written report

Physical Therapy

- Our current two traveling therapists, Lydia Peters and Chelsea Marcelle, will no longer be with the department as of 2/15/19.
- We have a new traveling physical therapist, Aimee Dosch, whom will join our dept. from 3/11/19-6/8/19.
- Progress towards manager goal of permanent recruitment: working on registration to CPTA (California Physical Therapy Association) Student Conclave at University of the Pacific, in Stockton, CA on 4/13/19.

Telemedicine

- Neurology clinic started with the first clinic on Tuesday, November 27, 2018.
- Current total visits starting July 2018 = 145 (55.8% of goal of 260)
- 305 total consults completed since the start of the program.

Respiratory Therapy

- No written report

Cardiac Rehab

- I have met with Val to brainstorm for a marketing plan to increase our attendance in Cardiac Rehab.
- We have reached out to MVHC to attend their provider meeting to let them know what Cardiac Rehab entails.
- I have worked on a presentation outline for the provider meeting.

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

ACCOUNTING OF DISCLOSURES

Synopsis of Policy: ***HIPAA Regulation:*** *Accounting for Disclosures § 164.528*

Individuals have the right to receive an accounting of disclosures of their protected health information made by a covered entity during the six years prior to the date that the individual requests the accounting, including disclosures to or by business associates. The right to an accounting only extends to "disclosures," i.e., sharing health information outside of the covered entity. It does not encompass "uses," i.e., using or sharing health information within the covered entity. For example, an individual would not have a right to a list of all hospital employees who have had access to his or her health information. The accounting must include the date of each disclosure; the name and, if known, the address of the entity or person who received the information; a description of the information disclosed; and a statement of the purpose of the disclosure. The covered entity must provide the individual with the accounting of disclosures no later than 30 days after it receives the request. The deadline may be extended up to an additional 30 days. The first accounting provided to an individual in any 12-month period is free.

The regulation specifically includes provisions that apply when the covered entity discloses the protected health information of 50 or more people in connection with a research project. These provisions allow the covered entity to include general information about such research-related disclosures whether or not the protected health information of the individual who requested the accounting actually was disclosed. There are a few exceptions to the individual's right to receive an accounting of disclosures, and they are specified in the regulation. For example, [the covered entity is not required to provide an accounting of disclosures that have been made to carry out treatment, payment, and health care operations. In effect, this means that patients do not have a right to know the names of everyone who has seen their records. They will not know who has seen their records in the course of providing or paying for care. The regulation also exempts from the accounting requirement disclosures made pursuant to an authorization and disclosures that are part of a limited data set. The covered entity must also temporarily suspend the individual's right for disclosures made to a health oversight agency or law enforcement official if the agency or official provides the covered entity with a statement indicating that providing the individual an accounting of the disclosure would reasonably likely impede agency activities. The statement must specify the suspension time required.

POLICY:

To ensure patients can receive an accounting of disclosures of their protected health information, not including disclosures for purposes of treatment, payment or health care operations. Disclosures to business partners must be included in the accounting. Under the Health Insurance Portability and Accountability Act, **Mayers Memorial Hospital District** must give patients an accounting of disclosures, if requested. Patients may request an accounting of disclosures that were made up to six years prior to the date of request.

PROCEDURES:

1. Maintain an accounting of disclosures of protected health information on each patient for at least six years or more if required by your individual state.

2. Information that must be maintained (tracked) and included in an accounting:
    A. Date of disclosure;
    B. Name of individual or entity who received the information and their address, if known;
    C. Brief description of the protected health information disclosed;
    D. Brief statement of the purpose of the disclosure (or a copy of the individual's written authorization) or a copy of the individual's written request for disclosure; and
    E. Multiple disclosures to the same party for a single purpose (or pursuant to a single authorization) may have a summary entry. A summary entry includes all information (2 A–E) for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.

3. Information that is excluded from the accounting and tracking rule(s) are disclosures made:
    A. Prior to April 14, 2003 or prior to Mayers Memorial Hospital District's date of compliance with the privacy standards;
    B. To law enforcement or correctional institutions as provided in State law;
    C. For facility directories;
    D. To the individual patient;
    E. For national security or intelligence purposes;
    F. To people involved in the patient's care;
    G. For notification purposes including identifying and locating a family member; and
    H. For treatment, payment, and healthcare operations pursuant to an individual's authorization.

4. All other disclosures of protected health information must be tracked. Disclosures are not limited to hard-copy information but any manner that divulges information, including verbal or electronic data release.

5. Disclosures may be tracked by a variety of internal processes that ensure accurate and complete accounting of disclosures, such as:
    A. Computerized tracking systems that have the ability to sort by individual and/or date;
    B. Manual logs with one log per patient maintained in the patient's health record; and
    C. Authorization forms maintained in the patient's health record.

6. All systems must be maintained and accessible for a period of at least six years to meet the requirement of providing an accounting of disclosures for that time period.

7. Disclosures that are not accompanied by a written request must be tracked by alternative computerized or hard-copy mechanisms.

8. A patient may make the request for an accounting in writing or orally. If the request is made orally, the organization should document such on the general "Authorization" form or a "Request for an Accounting of Disclosures" form. The organization must retain this request and a copy of the written accounting that was provided to the patient, as well as the name/departments responsible for the completion of the accounting.

9. A patient may authorize in writing that the accounting of disclosures be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).

10. Provide the individual with an accounting of disclosures within 60 days after receipt of the request.
    A. If the accounting cannot be completed within 60 days after receipt of the request, provide the individual with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
    B. Requests can cover a period of up to six years prior to the date of the request.

11. Provide the accounting to the individual at no charge for a request made once during any twelve-month period. A reasonable fee can be charged for any additional requests made during a twelve-month period provided that the individual is informed of the fee in advance and given an opportunity to withdraw or modify the request.

12. Maintain written requests for an accounting and written accountings provided to an individual for at least six years from the date it was created.
    A. Maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years, or as long as your state requires.

REFERENCES:
HIPAA Regulation: Accounting for Disclosures § 164.528

COMMITTEE APPROVALS
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

ASSIGNEED SECURITY RESPONSIBILITY

Synopsis of Policy: ***HIPAA Regulation:****164.308(a)(2) Assigned security responsibility*

At all times Mayers Memorial Hospital District shall have one individual identified and assigned to HIPAA security responsibility.

The HIPAA Security Officer is responsible for the oversight of Security Rule implementation by department and has the ultimate responsibility for ensuring HIPAA Security Rule policies are implemented and followed. Responsibilities include:

1. *Ensure that the necessary and appropriate HIPAA related policies are developed and implemented to safeguard the integrity, confidentiality, and availability of Electronic Protected Health Information (ePHI) within Mayers Memorial Hospital District.*

2. *Ensure that the necessary infrastructure of personnel, procedures and systems are in place:*
    a. *To develop and implement the necessary HIPAA related policies.*
    b. *To monitor, audit and review compliance with all HIPAA related policies.*
    c. *To provide a mechanism for reporting incidents and HIPAA security violations.*

3. *Act as a spokesperson and single point of contact for Mayers Memorial Hospital District in all issues relating to HIPAA security.*

4. *The job title and duties shall be documented further within the Full Policy found below.*

Definitions

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.

- Business Associate: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

    - ePHI: Electronic/Protected health information means individually identifiable health information:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.
- Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

At all times Mayers Memorial Hospital District shall have one individual identified and assigned to HIPAA security responsibility.

POLICY:

The HIPAA Security Officer is responsible for the oversight of the Security Rule and its implementation. They also have the ultimate authority and responsibility for ensuring HIPAA Security Rule policies are implemented and followed.

Responsibilities include:

1. Ensuring that the necessary and appropriate HIPAA related policies are developed and implemented to safeguard the integrity, confidentiality, and availability of electronic protected health information (ePHI) within Mayers Memorial Hospital District.

2. Ensuring that the necessary infrastructure of personnel, procedures, and systems are in place:
    a. To develop and implement the necessary HIPAA policies;
    b. To monitor, audit and review compliance with all HIPAA policies; and
    c. To provide a mechanism for reporting incidents and HIPAA security violations.

3. Act as a spokesperson and single point of contact for Mayers Memorial Hospital District in all issues relating to HIPAA security.

4. The job title and duties shall be documented within the Security Officer's Job Description.

Responsibilities:

The above HIPAA Security Officer responsibilities are assigned to the IT Security Officer for Mayers Memorial Hospital District. Mayers Memorial Hospital District ’s current Security Officer is identified as Chris Broadway who is the person that is responsible as the Security Officer.

The HIPAA Security Officer shall carry out the assigned responsibilities in coordination with their Job Description.

REFERENCES:
HIPAA Regulation: 164.308(a)(2) *Assigned security responsibility*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

AUTHENTICATION & PASSWORD MANAGEMENT

Synopsis of Policy: ***HIPAA Regulation:*** *164.312(d); 164.308(a)(5); 164.312(a)(1)*

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A compromised password may result in a security breach of Mayers Memorial Hospital District's network. All Mayers Memorial Hospital District workforce members are responsible for taking the appropriate steps, as outlined in the full policy, to select and secure their passwords.

This policy reinforces the use and importance of effective passwords, also known as strong passwords. This policy will also require workforce members to change their passwords on a regular basis.

Information systems used to access ePHI shall uniquely identify and authenticate workforce members.

The policy specifies:
Standards of Authentication – Verification
The rules for maintaining ***Unique User ID and Password Management***
The guidelines for appropriate ***User ID and Passwords***

DEFINITIONS:

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.
- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
- Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

Passwords are an important aspect of computer security and are the front line of protection of user accounts. A compromised password may result in a security breach of Mayers Memorial Hospital District 's network. All Mayers Memorial Hospital District workforce members are responsible for taking the appropriate steps to select and secure their passwords. The purpose of this policy is to reinforce the use of effective passwords, also known as strong passwords, and require workforce members to change their passwords on a regular basis.

POLICY:

Information systems used to access ePHI shall uniquely identify and authenticate workforce members.

Authentication – Verification

Industry standard protocols will be used on all routers and switches used in the Wide Area Network (WAN) and the local area networks (LANs). Authentication types can include:

1. Unique user ID and passwords
2. Biometric identification system
3. Telephone callback
4. Token system that uses a physical device for user identification
5. Two forms of authentication for wireless remote access
6. Information systems used to access ePHI shall identify and authenticate connections to specific devices involved in system communications (digital certificate, for example)

The password file on the authenticating server shall be adequately protected and not stored unencrypted.

Unique User ID and Password Management

1. All Mayers Memorial Hospital District workforce members are assigned a unique user ID to access the network. All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.

2. Upon receipt of a user ID, the person assigned to said ID is required to change the password provided by the administrator to a password that only he or she (the user) knows. Effective passwords shall be created in order to secure access to electronic protected health information (ePHI).

3. Workforce members who suspect that their password has become known by another person shall change their password immediately. No user shall give his or her password to another person.

4. Workforce members are required to change their network user ID passwords every six months; when the technology is capable. Each application access password shall be changed every six months. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords every six months.

5. All privileged system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) shall be changed at least each fiscal quarter. All passwords are to be treated as sensitive, confidential Mayers Memorial Hospital District information.

User ID & Password Guidelines

Where possible, implement unique user IDs that are different from the e-mail address; Mayers Memorial Hospital District is encouraged not to use standard naming conventions for user IDs and should avoid using the same email user name as the system user ID.

1. Password length:
   a. 8-character passwords are the absolute minimum;
   b. 10-12 characters or longer is recommended; and
   c. Passwords up to 64 characters should be allowed.

2. Requiring mixed case, numbers, or special characters is recommended

3. Requiring users to periodically change their passwords is recommended:
   a. Every 6 months or a year preferably.
   b. Passwords are required to change if there is a suspicion that a password has been compromised.
4. Password selection software should not allow "obvious" passwords:
   a. Common words, words related to the user, repeated letters, numeric sequences, etc. (e.g, "password123", "johnsmith", or "abcabcabc").

5. Login software should include features to prevent brute force attacks, such as:
   a. Delays between login attempts; and
   b. Lock account after a number of failed attempts.
6. Password protection requirements for users:
   a. Never reveal a password over the phone to anyone;
   b. Never reveal a password in an email message;
   c. Never reveal a password to your supervisor;
   d. Never talk about a password in front of others;
   e. Never hint at the format of a password (e.g., "my family name");
   f. Never reveal a password on questionnaires or security forms;
   g. Never share a password with family members;

h. Never reveal a password to co-workers;
i. Never write down your password; instead, memorize it;
j. Never keep a list of user IDs and passwords in your office; and
k. Never misrepresent yourself by using another person's user ID and password.

Policy Responsibilities:

Managers and Supervisors Responsibility
Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing'.

IT Team(s) Responsibilities for Network User ID Creation

1. System administrators shall provide the password for a new unique user ID to only the user to whom the new ID is assigned.

2. Workforce members may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its attempted use at log on so that the user is required to change the provided password to one only they know.

All Workforce members accessing ePHI
Any workforce member who suspects that their password has become known by another person shall change their password immediately.

PROCEDURES

Managers and Supervisors Responsibility
Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing'. If access to another worker's account is required, managers/supervisors shall follow the emergency access section of Mayers Memorial Hospital District 's HIPAA User Access Management policy.

IT Team(s) Responsibilities for Network User ID Creation

1. System administrators shall provide the password for a new unique user ID to only the user whom the new ID is assigned.

2. Workforce members may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one only they know.

All Workforce Members Accessing ePHI

Any workforce member who suspects that their password has become known by another person shall change their password immediately.

REFERENCES:
HIPAA Regulation: 164.312(d); 164.308(a)(5); 164.312(a)(1)

COMMITTEE APPROVALS:
HIM/HIIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

CONSTRUCTION CHANGE ORDERS POLICY

POLICY:

The Board recognizes that during any construction project, unanticipated conditions or extenuating circumstances may develop, which by their nature require decisions within a short period of time in order to prevent costly delays and other negative circumstances. Therefore, the Board of Directors for Mayers Memorial Hospital District delegates approval of change orders to construction contracts as follows:

Chief Executive Officer

A change order that has been reviewed and approved by the Chief Financial Officer and the Chief Operating Officer, and has a total cost of less than $100,000, may be approved by the Chief Executive officer if the change order meets the following conditions:

A description and justification for the requested change(s) in relation to the original bid specifications, the general contractor's summary of total costs and/or credits to affect the change order and any required documentation to update the districts records/files is provided.

The change order does not significantly alter the approved contract

The approval of the change order is necessary to ensure the project remains within its timeline.

The purpose of the change order is to address a previously unknown condition and is not for what would otherwise be additional work.

The board Finance committee has been notified if the change order will be over $50,000.

Board of Directors

Any change order that exceeds the approval level of the Chief Executive Officer, or significantly alters the original contract, shall be approved by the Board of Directors at a Regular or Special Meeting prior to proceeding with the items of the change order. Prior to presenting the change order to the Board for approval, the following must occur:

The change order must be approved by the Chief Financial Officer, Chief Operating Officer, and the Chief Executive officer.

A description and justification for the requested change(s) in relation to the original bid specifications, the general contractor's summary of total costs and/or credits to affect the change order and any required documentation to update the districts records/files.

Emergency Change Orders

Should a condition arise that is deemed an emergency or an imminent threat to the safety of employees of the District or the contractors, the general public, or the structural integrity of the facility, a change order may be approved by the Chief Executive Officer, with the verbal consent of the Board President, should the amount exceed the Chief Executive Officers authorized approval. All such Emergency Change Orders must be reviewed by the Chief Operating Officer and Chief Financial officer and details shall be provided to the full board as soon as the documents become available.

COMMITTEE APPROVALS:
P&P: 6/7/2018
MEC: 10/24/1028

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

CONSULTATION – OCCUPATIONAL THERAPY

RESTORATIVE PROGRAMS:

- Rehabilitation Services' goal shall be to provide the highest services to all patients who need assistance in achieving their maximum independent functioning.

- To implement this goal, the Occupational Therapist must be very involved in the operation, not only with those patients directly receiving occupational therapy services, but indirectly with all patients in the hospital by attending staff meetings, giving input and staff education to the Restorative Nurse Aid program and by being available for consultation on an informal basis at all times. An Occupational Therapist can advise on necessary adaptive equipment and information on achieving maximum independence for individuals and recommendations for review in RNA programs for specific patients.

- The Occupational Therapist shall be especially valuable in assisting the Nursing Department and developing and monitoring the restorative dining program on an ongoing basis.

HOSPITAL INSERVICES:

- Inservice programs requested by other departments, such as Food and Nutrition Services, Environmental Services, Physical Therapy, shall be provided by Occupational Therapist, as requested.

- Training/inservice programs shall include, but not be limited to, the following topics:

    - Self-care techniques
    - Positioning for bed, wheelchair or feeding
    - Proper body mechanics for patient care
    - Improving the hospital’s feeding program
    - Bowel and bladder programs
    - Specific diseases or disabilities and Occupational Therapist’s role (CVA, arthritis, Parkinson’s)

- Methods to assist with confusion/reality orientation
- Joint protection techniques
- How energy conservation/work simplification techniques help disabled individuals accomplish ADLs
- Low vision or blind techniques
- Adaptations to the patient's environment; how this can increase functional independence
- Use of assistive devices for ambulation, transfers, eating and dressing
- Care and maintenance of assistive devices
- Design and fabrication of splints and slings
- Compensatory techniques for perceptual-motor dysfunction
- Therapeutic exercise and activities for strengthening arms and hand muscles

COMMITTEE APPROVALS:
M/P&T: 1/24/2019

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

CONTINGENCY PLAN and DISASTER RECOVERY

Synopsis of Policy: ***HIPAA Regulation:*** *164.308(a)(7) Contingency plan, Data backup plan, Disaster recovery plan, Emergency mode operation plan, Testing and revision procedures, Applications and data criticality analysis; 164.310(a)(1) Contingency operations*

This policy sets forth rules for continuing business without the normal resources of Mayers Memorial Hospital District (MMHD). These include the required procedures for an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:

- *Applications and data criticality analysis*
- *Data backup*
- *Disaster Recovery Plan*
- *Emergency mode operation plan*

The policy details specific requirements for each of these critical functions, and the responsibility for the creation, evaluation, testing and updating of the various contingency plans described therein.

DEFINITIONS:

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The purpose of this policy is to establish rules for continuing business without the normal resources of MMHD

POLICY:

1. MMHD shall develop procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:
   a. Applications and data criticality analysis;
   b. Data backup;
   c. Disaster Recovery Plan; and
   d. Emergency mode operation plan.

2. Each of the following plans shall be evaluated and updated at least annually as business needs and technology requirements change.

Applications and Data Criticality Analysis

1. MMHD shall assess the relative criticality of specific applications and data within MMHD for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
2. MMHD shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
3. The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup Plan

1. All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. ePHI shall not be saved on the local drives of personal computers.
3. ePHI stored on portable media (e.g. thumb drives, external hard drive, CD ROM Disks) shall be saved to the network to ensure backup of ePHI data.
4. MMHD shall conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.
5. MMHD shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI.
6. The Data Backup Plan shall apply to all files that may contain ePHI.
7. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility. Or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it usually backs up.

8. If a non-MMHD off-site storage facility or backup service is used, a written contract shall be used to ensure that the contractor shall safeguard the ePHI in an appropriate manner.
9. Data backup procedures outlined in the Data Backup Plan shall be tested on, at least, an annual basis to ensure that exact copies of ePHI can be retrieved and made available.
10. MMHD shall submit its new and revised Data Backup Plan to the Compliance Officers for approval.

Disaster Recovery Plan

1. To ensure that MMHD can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing ePHI. MMHD shall establish and implement a Disaster Recover Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner. The Disaster Recovery Plan for MMHD shall be incorporated into MMHD**'s** Disaster Recovery Plan.
2. The Disaster Recovery Plan shall include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
3. The Disaster Recovery Plan shall include procedures to log system outages, failures, and data loss to critical systems. Also, procedures will be implemented to train the appropriate personnel in regards to the disaster recovery plan.
4. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all time(s), who shall be trained to implement the Disaster Recovery Plan.
5. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.
    a. MMHD shall submit its new and revised Disaster Recovery Plan to the Compliance Officers for approval.

Disaster and Emergency Mode for Small Practices (Larger Organizations like Clinics and Hospitals should use the Full Disaster Recovery Plan)

1. Real Estate/Office Suite: Who to call, Phone Number
2. Computers: Who to call, Phone Number
3. Networking of Computers: Who to call, Phone Number
4. Restoration of Data to Server or Connection to the Internet: Who to call, Phone Number
5. EHR Support: Who to call, Phone Number
6. Add anything else needed to continue business

Emergency Mode Operation Plan

1. MMHD shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves critical business processes that shall occur to protect the security of electronic protected health information during and immediately after a crisis situation.
2. Emergency mode operation procedures outlined in the Disaster Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
3. MMHD shall submit its new and revised Emergency Mode Operation Plan to the Compliance Officers for approval.

Policy Responsibilities:

The Compliance/Security Officer shall oversee the creation, evaluation, testing, and updating of the various contingency plans described herein.

MMHD shall submit its new and/or revised procedures and plans to the Security Officer for approval and ongoing evaluation. Any procedures developed by MMHD shall be consistent with MMHD HIPAA policies and not deviate from MMHD standards.

REFERENCES:

- 164.308(a)(7) *Contingency plan*
- 164.308(a)(7) *Data backup plan*
- 164.308(a)(7) *Disaster recovery plan*
- 164.308(a)(7) *Emergency mode operation plan*
- 164.308(a)(7) *Testing and revision procedures*
- 164.308(a)(7) *Applications and data criticality analysis*
- 164.310(a)(1) *Contingency operations*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

DEVICE and MEDIA CONTROLS

Synopsis of Policy: ***HIPAA Regulation:*** *164.310(d)(1) Device and media controls; Disposal; Media reuse; Accountability; Data backup and storage*

This policy is to ensure that Electronic Protected Health Information (ePHI) stored or transported on storage devices is appropriately controlled and managed. Examples include thumb drives, external hard-drives and removable media.

This policy details Device and Media Controls and outlines responsibility for their accountability.

The policy details implementation specification(s) for:

- *Portable Media Use & Security*
- *Disposal*
- *Media Reuse*
- *Sending a Computer Server or Hard-Drive out for Repair*
- *Moving Computer Server Equipment with ePHI*
- *Device and media acquisition*

The policy specifies the various responsibilities of:

- *Manager/supervisor*
- *IT*
- *Workforce for Device and Media controls*

DEFINITIONS

- Covered Entity: A health plan or a health care provider that stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate: Any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization which, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.
- ePHI: Electronic/Protected Health Information is any individually identifiable health information:
  - Transmitted by electronic media;

- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.
- Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The intent of this policy is to ensure that ePHI stored or transported on storage devices and removable media is appropriately controlled and managed.

POLICY:

Device and Media Controls/Accountability

1. Mayers Memorial Hospital District (MMHD) shall protect all hardware and electronic media that contains electronic protected health information (ePHI). This includes personal computers, PDAs, laptops, storage systems, backup tapes, CD ROM disks, and removable disks.

2. Every area of MMHD is responsible for developing procedures that govern the receipt and removal of hardware and electronic media that contain(s) ePHI into and out of a facility. Procedures shall include maintaining a record of movements of hardware and electronic media and any persons responsible.

Portable Media Use - Security

1. In addition to protecting MMHD's workstations and facilities, workforce members shall protect ePHI when working from all other locations. This includes locations such as home, other offices, or when working in the field.

2. In order to limit the amount of portable ePHI, workforce members shall not save any ePHI on CD ROM Disks and other portable items.

3. Methods for protecting portable media with ePHI include:
   a. All workforce members shall receive permission from their supervisor before removing ePHI from their facility. Approvals shall include the type of permission and the time period for authorization. The time period shall be a maximum of one year.
   b. Workforce members who work in the field shall not leave ePHI unlocked or visible in their vehicles. They will also not leave any ePHI in client facilities/homes.
   c. If ePHI is lost, workforce members are responsible for promptly contacting their supervisor, the Security Officer or designated Compliance Officers responsible for HIPAA Compliance within one business day upon awareness that ePHI has been lost.

Disposal

1. Before electronic media that contains ePHI can be disposed, the following actions shall be taken on computers used in the workplace, at home, or at remote sites:
   a. Hard drives shall be either wiped clean or destroyed. Hard drive cleaning shall meet the Department of Defense (DOD) standards, which states, *"The method of destruction shall preclude recognition or reconstruction of the classified information or material."* In addition, the hard drive shall be tested to ensure the information cannot be retrieved.
   b. Backup tapes shall be destroyed or returned to the owner and their return documented. Destruction shall include a method to ensure there is no ability to reconstruct the data.
   c. Other media, such as memory sticks, USB flash drives or micro drives, CD-ROMs and floppy disks, shall be physically destroyed (broken into pieces) before disposing of the item.

Media Reuse

1. All ePHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the ePHI, or when the equipment is transferred to a new worker with different ePHI access needs. Hard drives shall be wiped clean before transfer.

2. Cleaning shall meet the Department of Defense (DOD) standards, which states, *"The method of destruction shall preclude recognition or reconstruction of the classified information or material."* In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

Sending a Computer Server Hard Drive to Repair

When the technology is capable, an exact copy of the ePHI shall be created and the ePHI removed from the server hard drive before sending the device out for repair.

Moving Computer Server Equipment with ePHI

Before moving server equipment that contains ePHI, a retrievable exact copy needs to be created.

Device and Media Acquisition

MMHD shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).

Policy Responsibilities:

Manager/Supervisor Responsibilities:

1. Ensure that only workforce members who require the need to remove ePHI from their facilities are granted permission to do so.

IT Responsibilities

1. Ensure all hard drives are wiped clean before disposal or reuse
2. Test hard drives to ensure they are clean
3. Before moving hardware or sending hard drives for repair that contains ePHI, create a retrievable copy of that data
4. Maintain an inventory and a record of movements or transfers of hardware and electronic media such as workstations, servers, or backup tapes

Workforce Responsibilities:

1. Individual workforce members or their units shall track Laptops, PDAs, CD ROM Disks, and floppy disks, and all other portable media that contain ePHI.
2. To limit the amount of portable ePHI, workforce members shall not save any quantity of ePHI onto floppy disks, CD ROMs and other portable items when it is not necessary.
3. Workforce members shall remove and destroy all ePHI before disposing of the media.

PROCEDURES

MMHD shall document written procedures to track, dispose, and reuse media devices used for ePHI. MMHD shall submit all new and revised procedures to the Security Officer for approval and ongoing evaluation. Any procedures developed by MMHD shall be consistent with MMHD **'s** HIPAA policies and not deviate from MMHD standard.

REFERENCES:

- 164.310(d)(1) *Device and media controls*
- 164.310(d)(1) *Disposal*
- 164.310(d)(1) *Media reuse*
- 164.310(d)(1) *Accountability*
- 164.310(d)(1) *Data backup and storage*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

EVALUATIONS – OCCUPATIONAL THERAPY

POLICY:

Patient assessment shall be the primary responsibility of the Registered Occupational Therapist with the Certified Occupational Therapy Assistant (COTA) contributing to the completion of the assessment process. The assessment process shall include the screening, evaluation and reassessment, and shall be documented in the patient's medical record.

PROCEDURE:

- The Registered Occupational Therapist shall establish the screening procedure to determine the extent of information necessary for collection.
    - The Certified Occupational Therapy Assistant may collect screening data and report it to the supervising Registered Occupational Therapist.
    - The Registered Occupational Therapist shall analyze, interpret and summarize the screening data and formulate a recommendation.
- The Registered Occupational Therapist shall identify the evaluation instruments, supervise the administration of the evaluation and analyzes, interpret and summarize the evaluation data to formulate a recommendation.
- The Certified Occupational Therapy Assistant, after demonstrating service competency, can participate in data collection, the administration of standardized and criterion referenced tests and the scoring of test protocols. The Certified Occupational Therapy Assistant shall not determine the information to be collected or the evaluation methodology. The Certified Occupational Therapy Assistant shall not perform skilled observations and unstructured tests.
- Reassessment shall be an on-going process of data collection and interpretation to provide the information to continue rehabilitation services.
- The Registered Occupational Therapist and Certified Occupational Therapy Assistant shall participate in the reassessment process.

- The following data may be collected by the Certified Occupational Therapy Assistant, with all data collection approved by the supervising Registered Occupational Therapist:
    - Patient name
    - Payer type (insurance type), ID number and group number
    - Medical history
    - Mental and cognitive/perceptual status
    - Assistance level of self-feeding, grooming/hygiene, bathing, dressing and all aspects of ADL
    - Adaptive equipment use
    - Functional mobility and transfer assistance level
    - Functional strength, range of motion of upper extremities, grip strength
    - Balance in sitting and standing
    - Strength and coordination

REFERENCE:

The American Journal of Occupational Therapy. (November/December 2014). Scope of Practice. Volume 68, S34-S40. Retrieved from http://ajot.aota.org/article.aspx?articleid=1934867

COMMITTEE APPROVALS
M/P&T: 1/24/2019

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

FACILITY ACCESS CONTROLS

Synopsis of Policy: HIPAA Regulation: 164.310(a)(1) Facility security plan; Facility access controls; Access control and validation procedures; Maintenance records; Contingency operations

This policy establishes protocols for securing facilities that contain Electronic Protected Health Information (ePHI).

Mayers Memorial Hospital District (MMHD) shall reasonably safeguard ePHI from any intentional or unintentional use or disclosure MMHD shall protect its facilities where ePHI can be accessed.

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Compliance Officers to ensure the facility plan components below are compliant with the HIPAA Regulations.

MMHD shall safeguard its facilities and the equipment therein from unauthorized physical access, tampering and theft. MMHD 's Compliance Officers shall annually audit facilities to ensure that ePHI safeguards are continuously being maintained.

The policy details implementation specification for:

- *Visitor Access Control:*
- *(IF YOU HAVE) Security Access Cards:*
- *(IF YOU HAVE) Keypads/Cipher Locks:*
- *Metal/Hard Keys:*
- *Network Closet(s):*
- *Server Room(s):*
- *Alarm System(s):*
- *Doors:*
- *Contingency Operations - Emergency Access to Facilities*
- *Maintenance Records Policy - For all sites that access ePHI*

DEFINITIONS

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.

- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity,

performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The intent of this policy is to establish protocols for securing facilities that contain ePHI.

POLICY:

General
MMHD shall reasonably safeguard electronic protected health information (ePHI) from any intentional or unintentional use or disclosure. MMHD shall protect its facilities where ePHI can be accessed.

New or Remodeled Facility in MMHD
When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Compliance Officers to ensure the facility plan components below are compliant with the HIPAA Regulations.

Facility Security Plan
MMHD shall safeguard the facilities of MMHD and the equipment therein from unauthorized physical access, tampering, and theft. MMHD Compliance Officers shall annually audit MMHD's facilities to ensure ePHI safeguards are continuously being maintained.

Facility security guidelines for the workforce:

a. Do not share access cards to enter the facility;
b. Do not allow other persons to enter the facility by "piggy backing" *(entering the facility by walking behind an authorized person, through a door without using a card in the reader);*
c. Do not share hard key access to enter the facility; and
d. Do not share alarm codes or keypad codes to enter the facility.

One or more of the following shall be implemented for all sites that access ePHI:

1. **Visitor Access Control:** In facilities where ePHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls. These procedures may vary depending on the facilities structure, the type of visitors, and where the ePHI is accessible.

4. **Metal/Hard Keys:** Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:
    a. Clearances based on programmatic need, special mandated security requirements and workforce member security; and
    b. A mechanism to track which workforce members are provided access

5. **Network Closet(s):** Every network closet shall be locked whenever the room is unoccupied or not in use. MMHD shall document who has access to the network closets and periodically change the locking mechanism to these closets.

6. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use. MMHD shall document who has access to each server room and periodically change the locking mechanism to server rooms.

7. **Alarm Systems:** All buildings that have ePHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members that require this information in order to leave and enter a building. These alarm codes shall be changed at least every six months.

8. **Doors**: All external facility doors and doors to areas where ePHI is housed shall remain completely shut at all times. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the vicinity. Sometimes the doors do not completely close by themselves. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

Contingency Operations - Emergency Access to Facilities

Each facility shall have emergency access procedures in place that allow facility access to appropriate persons to access data. This includes a primary contact person and back-up person for when facility access is necessary after business hours by persons who do not currently have access to the facility.

Maintenance Records Policy

Repairs or modifications to the physical building for each facility where ePHI can be accessed shall be logged and tracked. These repairs are tracked centrally by General Services – Facility Management. The log shall include events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

Policy Responsibilities:

Manager/supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the facility plan;

2. Authorize clearances that are appropriate to the duties of each workforce member;
3. Notify the security administrator or designee within one business day when a user no longer requires access to the facility; and
4. Verify that each worker surrenders her/his card or key upon leaving employment.

Worker Requirements:

1. Display their access/security card to demonstrate their authorization to access restricted areas;
2. Immediately report lost or stolen (key/ID) cards, or metal keys or keypad-cipher lock combinations; and
3. Surrender access card or key upon leaving employment.

Facility Manager/Security Officer or Designee Requirements:

1. Request and track maintenance repairs;
2. Establish and maintain a mechanism for accessing the facility in an emergency;
3. Track who has access to the facility;
4. Change metal locks when a key is lost or unaccounted for;
5. Change combination keypads/cipher locks every three months;
6. Change the alarm code every six months;
7. Disable access cards not used for 90 days or more; and
8. Complete access card audits every 6 months to verify user access.

Security Officer responsibilities:

1. Work with General Services and MMHD to ensure facilities comply with the HIPAA Security Rule for facility access controls; and
2. Conduct annual audits of MMHD's facilities to ensure the facility is secured and the requirements of this policy are being enforced.

PROCEDURES

MMHD shall document written procedures for their facility security plan. Procedures shall be written to address the unique requirements of each facility. An essential part of compliance is to document and implement processes to ensure the safeguards in the facility security plan are being maintained.

MMHD shall submit new and revised procedures and plans to the Compliance Officers for approval and ongoing evaluation. Any procedures developed by MMHD shall be consistent with MMHD's HIPAA policies and not deviate from MMHD standard.

REFERENCES:
HIPAA Regulation:

- 164.310(a)(1) *Facility security plan*
- 164.310(a)(1) *Facility access controls*
- 164.310(a)(1) A*ccess control and validation procedures*
- 164.310(a)(1) *Maintenance records*
- 164.310(a)(1) *Contingency operations*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

2018 HHS POVERTY GUIDELINES

Persons in Family or Household	75% US Poverty Level
1	$ 9,105
2	$ 12,345
3	$ 15,585
4	$ 18,270
5	$ 22,065
6	$ 25,305
7	$ 28,545
8	$ 31,785
For each add'l person, add	$ 3,240

To determine charity eligibility according to income level:

1. Count the number of persons in your family/household
    a. For persons 18 years of age and older, include spouse, domestic partner and dependent children under 21 years of age, whether living at home or not
    b. For persons under 18 years of age, include parent, caretaker relatives and other children under 21 years of age of the parent or caretaker relative
2. Calculate the household income
3. On the row corresponding to the number of persons in your family/household above, compare your household income to the amount in the column labeled "75% US Poverty Level"
4. If your household income is less than 75% US Poverty Level amount, your income supports your eligibility for Charity Care.

Note: Pursuant to AB 774 Sect. 127405(2), Mayers Memorial Hospital has established eligibility levels for financial assistance and charity care at less than 350 percent of the federal poverty level as appropriate to maintain its financial and operational integrity. Mayers Memorial Hospital is a rural hospital as defined in Section 124840.

To determine charity eligibility according to total monetary assets:

1. Calculate your total monetary assets (referred to as "ASSETS" in the equation below)
    a. Assets included in retirement or deferred-compensation plans qualified under the Internal Revenue Code, or nonqualified deferred-compensation plans **shall not** be included
2. Insert total assets into the following equation:
    a. (ASSETS – 10,000)/2
3. If the remaining amount is less than $5,000, your total asset level supports your eligibility for Charity Care.

Approvals: BOD: 12/28/16
MMH388 Page 1 of 1

HHS POVERTY GUIDELINES – 75%

Attached to policy Charity Care Policy

MAYERS MEMORIAL HOSPITAL DISTRICT

POLIC AND PROCEDURE

JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

Synopsis of Policy: 164.512(e) Use and Disclosure of PHI for Judicial and Administrative Proceedings

To ensure that this organization's employees understand when and how to disclose a patient's personal health information (PHI) in relation to judicial and administrative proceedings.

There may be instances where a patient is involved with a legal proceeding, either conducted by a court of law, such as a state trial or federal district court, or a government agency such as the Department of Health and Family Services or the federal Centers for Medicare & Medicaid Services.

In these legal proceedings, lawyers, judges and others involved with the proceeding may contact the Mayers Memorial Hospital District (MMHD) to access the patient's PHI. Examples of health information these proceedings may require include information about a certain medical procedure the patient underwent to determine whether the procedure is covered under a health plan or the outcome of that procedure, results of blood or genetic tests in child custody or similar proceedings, medical records that document disabling conditions in discrimination cases, or health information that documents serious illnesses for conflicts pertaining to medical leave. These are only some examples of cases where health information may be sought in judicial or administrative proceedings; there are likely many more situations where PHI may be requested to be released.

DEFINITION:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

POLICY:

MMHD may disclose PHI in the course of any judicial or administrative proceeding:

a. In response to an order from a court or administrative tribunal; and
b. In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal.

PROCEDURE for disclosing PHI in response to a court/administrative order:

If MMHD receives an order from a court or administrative judge, then release only the PHI which the order expressly authorized to be disclosed.

PROCEDURE for disclosing PHI in response to a subpoena, discovery request or other lawful process (other than a court order):

MMHD may only release PHI in such instances if at least one of the following three events has occurred:

1. MMHD may release PHI if it receives ***written*** "satisfactory assurance" from the party requesting the information that reasonable efforts have been made by such party to ensure that the patient who is the subject of the PHI has been given notice of the request.
    a. "Satisfactory assurance" that the requesting party has tried to notify the patient of the PHI request means the following:
        i. The requesting party has given MMHD a *written statement and accompanying documentation* demonstrating that:
            1. The requesting party has made a good faith attempt to provide written notice to the patient (if the patient's location is unknown, documentation showing that a notice was mailed to the patient's last known address);
            2. The notice provided by the requesting party to the patient contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
            3. The time for the patient to raise objections to the court or administrative tribunal has passed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court's resolution.
2. MMHD may also release PHI to a requesting party if it receives ***written*** satisfactory assurance from the requesting party that reasonable efforts have been made by such party to secure a *qualified protective order*. A *qualified protective order* is an order of a court or administrative tribunal or a stipulation by the parties to the proceeding that prohibits the parties from using or disclosing PHI for any purpose other than the proceeding for which the information was requested and requires the parties to return the PHI (including all copies made) to the MMHD at the end of the proceeding.
    a. "Satisfactory assurance" in this instance means that MMHD has received from the requesting party a written statement and accompanying documentation demonstrating that:
        i. The parties to the dispute giving rise to the request for PHI have *agreed* to a qualified protective order and have presented it to a

court or administrative tribunal with jurisdiction over the dispute; or

ii. The requesting party has asked for a qualified protective order from such court or administrative tribunal.

3. We may release PHI to a requesting party even without satisfactory assurance from that party if we, the MMHD, either:
    a. Make reasonable efforts to provide notice to the patient about releasing his or her PHI, so long as the notice meets all of the following requirements:
        1. The notice is written and given to the patient (if the patient's location is unknown, we should establish documentation showing that a notice was mailed to the patient's last known address);
        2. The notice contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
        3. The time for the patient to raise objections to the court or administrative tribunal has lapsed and either no objections were filed, or all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court's resolution; or
    b. Seek a qualified protective order from the court or administrative tribunal or convince the parties to stipulate to such order.

REFERENCES:

- 45 CFR § 164.512(e)

COMMITTEE APPROVALS
HIM/HIPAA: 10/25/2018

Lead Apron Inspection

Date: _____

Apron ID# _____

Inspection:

Type: Visual _____ Tactile _____ X-Ray Imaging _____

Results: Satisfactory _____ Unsatisfactory _____

Performed By: _____

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURES

LEAD APRON POLICY

DEFINITION:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

POLICY:

The purpose of this policy is to ensure proper inspection and evaluation of lead aprons to ensure safety to patients and employees while in areas where x-radiation is being generated.
It is the policy of Mayers Memorial Hospital District (MMH) to provide a safe environment in areas where x-radiation is generated for diagnostic purposes and patient care.

PROCEDURE:

Lead aprons shall be checked annually for defects, such as holes, cracks, or tears. This check can be done by visual inspection, tactile evaluation (feeling the protective devices) and by x-ray imaging. A record of the date of the check, the type of check and who performed the inspection shall be kept for a minimum of five years.
If a defect is found at the time of the annual inspection or on any other occasion, the device shall be removed from service immediately.
Apron Rejection Criteria
Aprons can fail testing for many reasons; the following are the most common examples:

- Multiple small holes and cracks
- Large hole or crack
- Wearing out or thinning of the lead
- Velcro not in working order (can be repaired)
- Holes and cracks can be seen when the apron is checked using fluoroscopy or fluoro spot device

Fluoroscopic lead aprons are to be discarded if inspections determine:

- A defect greater than 15 square mm found on parts of the apron shielding critical organs (e.g., chest, pelvic area).
- A defect greater than 670 square mm along the seam, in overlapped areas, or on the back of the lead apron.

- Thyroid shields with defects greater than 11 square mm.

REFERENCES:
Stanford University Environmental Health & Safety, Radiation Protection Guidance Hospital Staff, General Workplace Safety Guidance: Lead Apron Inspection and Inventory Policy
Radiologic Health Branch – California Department of Public Health, Title 17

COMMITTEE APPROVALS:
P&P: 1/3/2019

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY & PROCEDURE

LIGHT DUTY OR LIMITED JOB ASSIGNMENTS

POLICY:

Mayers Memorial Hospital District supports a return to work program for employees injured on the job. When an injured worker can be released by the physician for modified work in their own position or when released to perform work in an unrelated function Human Resources shall make a reasonable effort to find meaningful work to be performed.

PROCEDURE:

Employee Responsibility:

Employees should inquire about any work restrictions placed on them and should request the treating physician to document any limitations or recommendations for modified work. The employee shall communicate to their supervisor/manager and the Human Resource department, in a timely manner, any work restrictions placed upon them and provide the required support documentation to the HR department.

Hospital Responsibility:

Upon notification of release for modified work or light duty, the Human Resource department shall first work with the employees department to determine if modified work is available. The employees treating provider shall be notified of the modified work arrangement, given a copy of the modified duties and requested to approve the modified work program.
In the event the return to work requires the employee to work in a position that is not a modification of their current position, the treating provider and the employee shall both be given a copy of the job description and approval of the treating provider shall be requested.

Compensation:

When an employee is placed in a modified continuation of their current position there shall be no change in their compensation. However, if the employee is assigned to a position other than described above, compensation shall be in

accord with the pay grade assignment of the position. In some cases this could result in an increase or decrease in the hourly rate of pay. Workers compensation insurance shall provide economic assistance within perimeters established by law for any employee working at a rate lower than the rate paid at the time of injury.

COMMITTEE APPROVALS:

Chiefs:

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

MINDRAY ULTRASOUND USE AND CARE

DEFINITIONS:

The Mindray M-7 is a bedside ultrasound machine that can be used for diagnostic procedures and/or placement of intravenous catheters for in-patient or outpatient visits

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

POLICY:

It is the policy of Mayers Memorial Hospital District (MMHD) to provide competent patient care through the use of the Mindray M-7 Diagnostic Ultrasound System.

PROCEDURE:

The Physician may use the M-7 in the Emergency Room as an adjunct assessment tool.
The nurse may use the M-7 in the placement of peripheral venous catheters or in the assessment of urinary retention.

After every use of the M-7 ultrasound system, it will be cleaned in accordance with the Radiology Department's Ultrasound Transducer (Probe) Cleaning Policy and Procedure.

The product being used is "SONO Ultrasound Wipes".
Cleaning and disinfecting the transducer:

1. Clean off gel prior to wiping with SONO Ultrasound Wipe. Take one cloth hand wipe down the lens and surrounding surface of the transducer. SONO Ultrasound Wipes are safe to use on all areas of the ultrasound equipment including the keyboard, trackball, touch screen and LCD screen.
2. Wrap the SONO Ultrasound Wipe around the transducer and leave the transducer in the holder to keep surface wet.
3. Leave transducer in holder while you prepare for the next patient. Keep wipe on transducer at least four (4) minutes, ten (10) minutes if disinfecting for Norovirus or Coronavirus.
4. Wipe down the cable after you are finished disinfecting the transducer head.

SPECIAL CONSIDERATIONS:

Users must have completed the basic competency and training before using the Mindray M-7, which is conducted by the Imaging Department Ultrasound Sonographer. The Sonographer will cover basic operation and settings, which are also found in the Mindray M-7 Operator's Manual.

REFERENCES:

Policy and Procedure: Ultrasound Transducer (Probe) Cleaning
Operator's Manual:
Mindray M-7/M-7T
Mindray Medical USA Corporation 8650 154th Ave NE, Redmond, Washington 98052

COMMITTEE APPROVALS:

P&P: 8/2/2018
MEC: 10/24/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

MONITORING & EFFECTIVENESS

Synopsis of Policy: HIPAA Regulation: 164.308(a)(1) Perform a periodic technical and non-technical evaluation, requiring a process for Security management, risk analysis and risk management)

This policy establishes periodic evaluations of Mayers Memorial Hospital District's (MMHD) compliance with HIPAA policies and procedures. Security assessments shall be conducted periodically to confirm continued compliance with security standards and specifications. Assessments will determine if security controls are correctly implemented, and, as implemented, are effective in their application.

The policy also establishes procedures for Change Management of systems governed by the HIPAA Security Rule. The policy specifies the need for Change Control, Change Notification, Change Implementation, Change Closure and Evaluation.

The policy also specifies management and workforce responsibilities for implementation.

DEFINITIONS

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.
- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The intent of this policy is to establish periodic evaluations on whether MMHD is complying with the HIPAA policies and procedures to effectively provide confidentiality, integrity and availability of electronic protected health information (ePHI). Security assessments shall be conducted periodically to determine continued compliance with security standards and specifications. Assessments are conducted to:

1. Determine if security controls are correctly implemented, and, as implemented, are effective in their application;
2. Ensure that HIPAA security regulations, policies, and directives are met; and
3. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

POLICY:

Risk Assessment & Management:
MMHD, along with the Security Officer, shall monitor the effectiveness of MMHD's ability to secure ePHI. In order to accomplish this, a risk assessment shall be conducted when:

1. New technology is implemented that either contains ePHI or is used to protect ePHI;
2. New facilities that maintain or house ePHI are designed;
3. Existing facilities that maintain or house ePHI are being remodeled or the design layout is being altered;
4. New programs, functions, or departments are added that affect the security of MMHD**;**
5. Security breaches are identified; and
6. Changes in the mode or manner of service delivery are made.

Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be documented and implemented.

Change Control
The primary goal of change management is to facilitate communications and coordinate all changes that may occur in the IT environment. These changes include, but are not limited to, the installation, update, or removal of network services and components, operating system upgrades, application or database servers and software.

Change Notification
1. For informational purposes, the Compliance Officers shall be notified of changes by email no less than 48 hours in advance.
2. Emergency Changes shall be communicated to the Compliance Officers as soon as is reasonable.

3. Any change that encounters difficulties that could adversely affect customers, patients, or clients shall be communicated to the Compliance Officers as soon as is reasonable.

Change Implementation
All non-emergency changes shall occur within the recognized downtime unless approved in advance by all affected parties or for inter-departmental changes as department procedures dictate.

Change Closure
The disposition of all changes shall be documented.

Evaluation
MMHD shall conduct an assessment of security controls at least annually to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. Technical and non-technical evaluations are to be conducted periodically to identify any new risks or to determine the effectiveness of the HIPAA Security Policies and Procedures. These evaluations include but are not limited to the following:

1. Random audit reviews of a facility's physical environment security;
2. Random audit reviews of workstation security;
3. Periodic, unannounced tests of the physical, technical, and administrative controls;
4. Assessment of changes in the environment or business process that may affect the HIPAA Security Policies and Procedures;
5. Assessment when new federal, state or local laws and regulations are passed that may affect the HIPAA Security Policies and Procedures;
6. Assessment of the effectiveness of the HIPAA Security Policies and Procedures when security violations, breaches or other security incidents occur; and
7. Assessment of redundancy needed in the network or servers for ePHI availability.

Policy Responsibilities:

Compliance Officers
HIPAA Compliance Officers:

1. Are responsible to coordinate with the Security Officers to conduct audits of covered component compliance with the HIPAA security rule;
2. Shall coordinate the production of procedures to implement this policy; and
3. Are responsible for providing tools and processes for assessing technical and nontechnical evaluations as part of MMHD's ongoing compliance efforts.

If assessments recommend changes to the HIPAA Policies and Procedures, the Compliance Officers are responsible for reviewing these changes and presenting them to management. If needed, the Compliance Officers will update the workforce training materials.

PROCEDURES

The Compliance Officers shall write procedures to ensure ongoing evaluation and assessments are completed to mitigate risks to ePHI.

REFERENCES:
HIPAA Regulation:

- 164.308(a)(1) *Perform a periodic technical and non-technical evaluation*
- 164.308(a)(1) *Security management process*
- 164.308(a)(1) *Risk analysis*
- 164.308(a)(1) *Risk management*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

USE AND DISCLOSURES FOR MARKETING

Synopsis of Policy: 164.508.a.3 Use and Disclosures for Marketing

It is the policy of Mayers Memorial Hospital District (MMHD) to secure an authorization to use or disclose protected health information (PHI) for marketing purposes in compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. [164.501, 164.508(a)(3)]

DEFINITIONS:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

1. Per 164.501, marketing is defined as:
   a. To make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service; or
   b. An arrangement involving a covered entity whereby PHI is disclosed by the covered entity in exchange for direct or indirect remuneration, so that the other entity or affiliate can make a communication that encourages the purchase or use of its own product or service.

2. The following are examples of situations that do not meet the definition of marketing:
   a. Communications that are merely promoting good health and not about a specific product or service does not meet the definition of "marketing." This includes: mailings reminding women to get an annual mammogram; information about how to lower cholesterol; mailing about new developments in health care; new diagnostic tools; or upcoming health or "wellness" classes, support groups, and health fairs. These *are* permitted and are *not* considered marketing.
   b. Communications about government-sponsored programs do not fall within the definition of marketing. There is no commercial component to communications about benefits available through public programs. MMHD is permitted to use/disclose PHI to communicate about eligibility for Medicare supplement benefits or SCHIP.
   c. MMHD may make communications in newsletter format without authorization so long as the content of such does not fit the definition of "marketing."

Exceptions to the Scope of Marketing Activities Where Authorization is Not Needed:

3. Marketing does not include:
   a. Oral or written communications that describe MMHD's network or covered services;
   b. Communications about treatment for the patient; or
   c. Communications about case management or care coordination, or recommendations of treatment alternatives and care options, including health care providers or settings of care.

4. The following are examples of these exceptions:
   a. MMHD can convey information to beneficiaries and members about health insurance products offered by MMHD that could enhance or substitute for existing health plan coverage. For example, if a child is about to age-out of coverage under a family's policy, this provision will allow the plan to send the family information about continuation coverage for the child. This does NOT extend to excepted benefits such as accident-only policies or to other lines of insurance.
   b. Doctors can write a prescription or refer an individual to a specialist for follow-up tests because these are communications about treatment.

POLICY

It is the policy of MMHD to secure an authorization to use or disclose protected health information (PHI) for marketing purposes in compliance with the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. [164.501, 164.508(a)(3)]

PROCEDURE for Authorization to Use or Disclose PHI for Marketing Purposes:

1. MMHD will obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:
   a. Face-to-face communication with the patient; or
   b. A promotional gift of nominal value provided by MMHD.

2. If the marketing involves MMHD receiving direct or indirect remuneration by a third party, the authorization will state that such remuneration is involved.

3. The following is an explanation of situations that require authorization:
   a. Notice of Proposed Rule Making (NPRM) clearly states that nothing in the Final Rule will permit MMHD to sell lists of patients or enrollees to third parties, or to disclose PHI to a third party for the independent marketing activities of the third party. For example, a pharmaceutical company cannot pay a provider for a list of patients with a particular condition, or taking a particular

medication and then use that list to market its own drug products directly to patients.

REFERENCES:

- 45 CFR 164.501and 164.508(a)(3)

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLIC AND PROCEDURE

MINORS RIGHTS

Synopsis of Policy: 164.524 Minors Privacy Rights

Additional information by State can be found here: https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law

Generally, the age in most states at which a minor obtains the right of access to their healthcare information is 18 because at that age the individual is no longer deemed a minor. Most state laws grant a minor the right of access to their healthcare information and this right often directs a minor's statutory right to consent to treatment; however, there are exceptions.

The federal Privacy Rule also grants a minor access to their healthcare information but as a standard, only through the consent of a legally authorized representative. The federal law does not provide for direct access by a minor under the age of majority. The federal Privacy Law delineates a process for interfacing the federal and state law when they are different. The federal law allows the state law to preempt and control when state law provides a greater right of access to the individual in relation to their healthcare information. Therefore, if your state has a law on Minority Access, that law will control when a minor is provided a greater right of access.

Federal law requires that healthcare providers have in place and implement policies and procedures to ensure patients' right to access, inspect and copy protected health information (§164.524). Under the federal Privacy Rule, an individual has the right to access their information in all but a limited number of situations. When federal law limits the right of access interface with state law is required and the law that provides the individual the greater right of access controls. For instance, the Privacy Rule allows denial of access to specific types of healthcare information with or without a review of denial. When a state law provides access to a minor or legally authorized individual and the Privacy Rule does not, state law will control.

The Privacy Rule defers to state law for the definition of a legal representative. State law generally recognizes the minor's parent, guardian or legal custodian as the legally authorized representative. However, a termination of parental rights or a denial of physical placement by a court of law will affect the status of a parent in relation to a minor. Therefore, it will be necessary to determine what law is controlling to determine who may be the legally authorized representative for a minor regarding access.

DEFINITIONS:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

Minor: A minor is a person under the age of 18 years and reliant upon parental support and control. Generally minors do not have the authority to grant consent or refuse care, with the exceptions outlined below.

Emancipated Minor: In many states, lawful marriage is the only circumstance that is statutorily recognized, as a general matter, as grounds for emancipation of a minor. Once emancipated, the minor obtains the legal capacity of an adult. The burden should be placed on the minor to show emancipation. If doubt exists regarding emancipation, parental consent should be secured in addition to the consent of the minor.

POLICY:

It is the policy of Mayers Memorial Hospital District (MMHD) to recognize the rights of minors and their parents, legal guardian, or other legally authorized representative to access, inspect and receive copies of their protected health information in compliance with state and federal regulations. In most states, minors have many rights with regard to consent to their own care in certain situations. However, it is important to understand that these rights may not extend to their ability to control access to their protected health information.

Minor Access:
A minor, or legally authorized representative, must make a request to a covered entity to access and inspect their protected health information. Whenever possible, this request shall be made in writing. The federal Privacy Rule allows the requirement of a written request for access as long as the individual has received notice of the written requirement in the "Notice of Privacy practices." The request for access may be documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record. The minor's rights to access should be determined based on the following statutory information and whether or not they are authorized to make the written request without parental/guardian consent.

Mitigating Circumstances:
The law of release of minor records is a matter of some ambiguity and controversy, particularly regarding the circumstances justifying allowing a minor to make decisions about disclosure of protected health information in the absence of parental consent, or to deny parental access to minor records. While the general rule is that parental consent is required until the patient is eighteen years of age, there may be extenuating circumstances justifying a variance from this rule. Legal counsel should be contacted for case-by-case determination of whether such circumstances are present.

Parental, Legal Guardian or Other Legally Authorized Representative Access:

1. A parent, legal guardian, or other legally authorized representative has the right to access a minor's protected health information on behalf of the minor, unless:

A. The statutes provide protection from access to the minor's protected health information;
B. The parent has been denied periods of physical placement with the minor; or
C. In the case of minors age 14 or older, the minor requests no disclosure of their mental health records.

2. A parent, legal guardian, or other legally authorized representative has the right to access a minor's protected health information on behalf of the minor, even where the parent or guardian's consent was not required for treatment, unless:
   A. The statutes provide protection from access to the minor's protected health information;
   B. The parent has been denied periods of physical placement with the minor; or
   C. In the case of minors age 14 or older, the minor requests no disclosure of their mental health records.

3. A healthcare provider reserves the right to limit disclosure of protected health information to a minor's parent or guardian if, in the provider's professional judgment, they believe the minor would be in imminent danger if the information was released.

4. The parent's right of access terminates when the minor becomes emancipated or reaches the age of majority. If doubt exists regarding emancipation, parental authorization should be secured in addition to the authorization of the minor. Once a minor becomes emancipated, or reaches the age of majority, the individual has the right to access and authorize the disclosure of protected health information. This includes access to and disclosure of information created while the individual was a minor.

Other Minors Issues:

5. The PHI of minors prior to an adoption process is not available for disclosure by the healthcare provider. Requests for access to the PHI of a minor prior to an adoption shall be referred to the state law on adoption. Requests for PHI post-adoption shall be processes in accordance with the organization's disclosure of PHI policies.

6. A healthcare provider may disclose a minor's/student's immunization information to a school or daycare upon written or verbal request. Parental or student permission is not required for disclosure. Immunization information may be provided between vaccine providers, including the local health department, without the consent of the parent or student.

7. Documentation of disclosure to the individual is required under some state laws. To maintain consistency and compliance in practice, it is recommended that the following be documented when disclosing healthcare information to the patient: the time and date of request, the name of the inspecting person, and the identity of the records released.

Federal Privacy Rule – Access and Denial of Access

An individual has the right to access their information in all but a limited number of situations, which include:

1. Psychotherapy notes;
2. Information compiled in anticipation of or use in a civil, criminal, or administrative action or proceeding;
3. Protected health information subject to the Clinical Laboratory Improvements Amendment (CLIA) of 1988; and
4. Protected health information exempt from CLIA, pursuant to 42 CFR 493.3(a)(2). In other words, protected health information generated by: 1) facilities or facility components that perform testing for forensic purposes; 2) research laboratories that test human specimens but do not report patient-specific results for diagnosis, prevention, treatment, or the assessment of the health of individual patients; or 3) laboratories certified by the National Institutes on Drug Abuse (NIDA) in which drug testing is performed that meets NIDA guidelines and regulations.

In the situations above, the covered entity may deny the individual access without providing an opportunity for review.

A covered entity may also deny an individual access without providing an opportunity for review when:

1. The covered entity is a correctional institution or a healthcare provider acting under the direction of the correctional institution and an inmate's request to obtain a copy of protected health information would jeopardize the individual, other inmates, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the inmate;
2. The individual, when consenting to participate in research that includes treatment, agreed to temporary denial of access to protected health information created or obtained by a healthcare provider in the course of research, and the research is not yet complete;
3. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirement of that law; and
4. The protected health information was obtained from someone other than a healthcare provider under a promise of confidentiality and access would likely reveal the source of the information.

A covered entity may also deny an individual access under the following circumstances, provided that the individual is given a right to have such denials reviewed:

1. A licensed healthcare professional has determined that the access is likely to endanger the life or physical safety of the individual or another person;
2. The protected health information makes reference to another person who is not a healthcare provider, and a licensed healthcare professional has determined that the access request is reasonably likely to cause substantial harm to such other person; and
3. The request for access is made by the individual's personal representative and a licensed healthcare professional has determined that access is reasonably likely to cause substantial harm to the individual or another person.

REFERENCES:
Section 45 CFR, Section 164.524.

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

SOCIAL MEDIA

Synopsis of Policy: Social Media

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, micro-blogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

DEFINITIONS:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

PROCEDURES:

The following principles apply to professional use of social media on behalf of Mayers Memorial Hospital District (MMHD) as well as personal use of social media when referencing MMHD.

1. Employees should be aware that is never acceptable to post to social websites any information regarding patients, their condition, their treatment plan, and that sanctions up to and including termination will occur.
2. Employees need to know and adhere to the [Company's Code of Conduct, Employee Handbook, and other MMHD policies] when using social media in reference to MMHD.
3. Employees should be aware of the effect their actions may have on their images, as well as MMHD'S image. The information that employees post or publish may be public information for a long time.
4. Employees should be aware that MMHD may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to MMHD or its employees, or its customers.
5. Although this is not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
6. Employees are not to publish, post, or release any information that is considered confidential or private. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or their supervisor.

7. Social media networks, blogs and other types of online content can generate press, media attention, or legal questions. Employees should refer these inquiries to authorized MMHD spokespersons.
8. If employees find that they encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
9. Employees should get appropriate permission before they refer to or post images of current (or former) employees, members, vendors, and suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks, or other intellectual property.
10. Social media use shouldn't interfere with employee's responsibilities at MMHD. MMHD computer systems are to be used for business purposes only. When using MMHD computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, MMHD blogs, and LinkedIn). However, personal use of social media networks, or personal blogging of online content is discouraged and could result in disciplinary action.
11. Subject to applicable law, after-hours online activity that violates [the MMHD Code of Conduct] or any other company policy may subject an employee to disciplinary action or termination.
12. If employees publish content after-hours that involves work or subjects associated with MMHD, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent MMHD positions, strategies, or opinions."
13. It is highly recommended that employees keep MMHD-related social media accounts separate from personal accounts, if practical.

COMMITTEE APPROVALS:
HIM/HIPAA 06-13-2018
MEC: 8-16-2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

SECURITY AUDIT CONTROLS

Synopsis of Policy:

The intent of this policy is to provide the authority for workforce members representing the Mayers Memorial Hospital District 's IT organizations to conduct a security audit on any computing resource of the Mayers Memorial Hospital District.

Activity reviews provide indications that implemented safeguards are working, or that safeguards are insufficient. Audits may be conducted to:

1. *Ensure integrity, confidentiality, and availability of information and resources*
2. *Investigate possible security incidents to ensure conformance to Mayers Memorial Hospital District 's IT and security policies*
3. *Monitor user or system activity where appropriate*
4. *Verify that software patching is being maintained at the appropriate security level*
5. *Verify virus protection is being maintained at current levels*

HIPAA Regulation:

- *Log-in monitoring*
- *Information system activity review*
- *Audit controls*

DEFINITIONS:

- Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.

PURPOSE:

The intent of this policy is to provide the authority for workforce members representing the Mayers Memorial Hospital District IT organizations to conduct a security audit on any computing resource of the Mayers Memorial Hospital District.

Activity reviews provide indications that implemented safeguards are working, or that safeguards are insufficient. Audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources;
2. Investigate possible security incidents to ensure conformance to Mayers Memorial Hospital District IT and security policies;
3. Monitor user or system activity where appropriate;
4. Verify that software patching is being maintained at the appropriate security level; and
5. Verify virus protection is being maintained at current levels

POLICY:

Log-in Monitoring

1. Mayers Memorial Hospital District has the right to monitor system access and activity of all workforce members.

2. To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately secured; the following login monitoring measures shall be implemented:
   a. A mechanism to log and document four or more failed log-in attempts in a row shall be implemented on each network system containing ePHI when the technology is capable.
   b. Login activity reports and logs shall be reviewed biweekly at a minimum to identify any patterns of suspicious activity.
   c. All failed login attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Security Officer or the designee for each Mayers Memorial Hospital District.
   d. To the extent that technology allows, any user ID that has more than four-repeated failed login attempts in a row shall be disabled for a minimum of 30 minutes.

Information System Activity Review – Audit Controls
To ensure that activity for all computer systems accessing ePHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, every application and system administrator or designee shall review audit logs, activity reports, or other mechanisms to document and manage system activity.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with ePHI shall be archived.
5. Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Policy Responsibilities:

System administrators, Security Officers are responsible to implement and monitor audit controls for all systems that contain ePHI.

PROCEDURES:

Mayers Memorial Hospital District shall submit all new and revised procedures to the Office of HIPAA for approval and ongoing evaluation. The Security Officer shall create audit control checklists and logs to assist with, and standardize, the audit function. Any procedures developed by Mayers Memorial Hospital District shall be consistent with the Mayers Memorial Hospital District HIPAA policies and not deviate from the Mayers Memorial Hospital District standard.

REFERENCES:
Implemented on recommendation of Bob Grant our professional HIPAA consultant and expert in the field.

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

SECURITY AWARENESS and TRAINING

Synopsis of Policy: ***HIPAA Regulation:*** *164.308(a)(5) Security awareness and training*

This policy ensures that all members of MMHD*'s workforce who can access Electronic Protected Health Information (ePHI) receive the necessary training in order to implement and maintain the HIPAA Security Policies and Procedures. The intent is also to prevent any violations of confidentiality, integrity or availability of ePHI. Since* ***Security Awareness Training*** *is key to eliminating* MMHD*'s exposure to both malicious threats and accidental errors and omissions, its components are specified in the policy, along with training frequency, record keeping, and ongoing reminders.*

Compliance with Texas Medical Records Privacy Act security awareness and training requirements (as noted above) are also fulfilled in this policy.

DEFINITIONS

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.
- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The intent of this policy is to ensure that all members of MMHD's workforce that can access to electronic protected health information (ePHI) receives the necessary training in order to implement and maintain the HIPAA Security Policies and Procedures. Also, the intent of this policy is to prevent any violations of confidentiality, integrity or availability of ePHI.

POLICY:

Security Awareness Training
Security awareness training is key to eliminating MMHD's exposure to both malicious threats and accidental errors or omissions.

System & Application Training
This policy sets forth a minimum standard for system and application security awareness to reduce MMHD's risk:

1. Proper uses and disclosures of the ePHI stored in the application;
2. How to properly log on and log off the application;
3. Protocols for correcting user errors;
4. Instructions for contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
5. Reporting a potential security breach.

HIPAA Security Training

1. All members of the workforce that are part of MMHD shall receive security training. The Compliance Officers will provide the training and materials.

    a. Worker Level Training: This training entails Security Policies and Procedures that directly affect workers.
    b. Managerial - Supervisory Training: This training entails all of the HIPAA Security Policies and Procedures and Management's role in enforcement and supervision.

2. All new workforce members are required to attend the appropriate training within 60 days of entering the workforce.

3. MMHD is required to ensure that all of their workforce members receive training.

Tracking Security Training:
MMHD training coordinator or designee shall enter their workforce members into The Guard to sign them up for the appropriate level of training.

HIPAA Security Reminders

1. The Compliance Officers shall develop and implement periodic security updates and issue reminders to MMHD's workforce. These security reminders shall be provided using any media that is most effective for MMHD (e.g. email, posters, newsletters, intranet site, etc.).

2. At a minimum, these reminders shall be provided on a quarterly basis.

Policy Responsibilities:

Compliance Officers are responsible for ensuring that all workforce members in their operational areas are trained no later than 30 days after entering their workforce. In addition, the Compliance Officers will have oversight responsibility to audit reports from The Guard to ensure required workforce member attendance. If needed, the Compliance Officers may require workforce members to attend more training if security incidents warrant this remedial action.

PROCEDURES

Mayers Memorial Hospital District (MMHD) shall document written procedures on how new workers are notified and sent to training.

MMHD shall submit its new and revised procedures and plans to the Compliance Officers for approval and ongoing evaluation. Any procedures developed by MMHD shall be consistent with MMHD HIPAA policies and will not deviate from MMHD standard.

REFERENCES:
HIPAA Regulation:

- 164.308(a)(5) *Security awareness and training*
- 164.308(a)(5) *Security reminders*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

SOLICITATION

POLICY:

It is the policy of Mayers Memorial Hospital District to prohibit solicitation and distribution on its premises by non-employees and to permit solicitation by employees only as outlined below.

PROCEDURE:

1. Mayers Memorial Hospital limits solicitation and distribution on its premises because those activities can interfere with its normal operations, reduce employee efficiency, annoy patients and visitors, interfere with the efficient delivery of care, and pose a threat to safety and security.

2. Individuals not employed at Mayers Memorial Hospital are prohibited from soliciting funds or signatures, conducting membership drives, distributing literature or gifts, offering to sell merchandise or services (except by representatives of suppliers properly identified by the Human Resource Department), or engaging in any other solicitation, distribution, or similar activity on Mayers Memorial Hospital premises.

3. Employees may not solicit visitors, medical staff members or patients. Examples of such activities are Tupperware, Avon, AMWAY, Mary Kay Cosmetics, etc.

4. Mayers Memorial Hospital District maintains various communication systems to communicate hospital information to employees and to disseminate or post notices required by law. These communication systems (including bulletin boards, electronic mail, intranet, voice mail, facsimile machines, and computer work stations) are for business use only and may not be used for employee solicitation or distribution of literature. The unauthorized use of communications systems or the distribution or posting of notices, photographs, or other material on any company property is prohibited.

5. Hospital employees, who offer goods and services to other employees for purposes of supplementing their own incomes, should not do so on hospital time.

6. The Mayers Auxiliary is the only organization that is authorized for retail sales in Fall River Mills and Burney.

7. Mayers Memorial Hospital may authorize a limited number of fund drives by employees on behalf of charitable organizations or for employee gifts. These activities require the approval of the Human Resource Director and the participation by employees is entirely voluntary.

8. Hospital sponsored and approved fund raising for the Mayers Intermountain Healthcare Foundation may be done on hospital time and hospital property but every effort should be made to avoid interfering with patient care during these activities.

9. The following restrictions apply when employees engage in permitted solicitation or distribution of literature for any group or organization, including charitable organizations:

    a. The sale of merchandise or services prohibited on hospital premises.
    b. Soliciting and distributing literature during the working time of either the employee making the solicitation or distribution or the targeted employee is prohibited. The term "working time" does not include an employee's authorized meal or rest periods or other times when the employee is not required to be working.
    c. Soliciting and distributing literature is prohibited in any patient care area.
    d. Distributing literature in a way that causes litter on hospital property is prohibited.
    e. Off-duty employees are not allowed to remain on or return to Mayers Memorial Hospital premises for the purposes of solicitation or distribution following their scheduled work hours.

10. Employees may submit information to Administration no later than the Monday before each payday to be approved and distributed to employees.

11. The Human Resource Department is responsible for administering this policy and enforcing its provisions. Employees who conduct home business activities that interfere with the primary mission of the hospital, caring for patients, may be asked to discontinue any activity at the hospital, or face disciplinary action.

COMMITTEE APPROVALS:
Chiefs Team: 1/4/2019

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

SWING INTAKE WORKSHEET

Page 1 of 1, plus the following Attachment
Swing Intake Worksheet, MMH613.

DEFINITION

Essentially, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

POLICY:

This document should be used by the acute social worker when putting intake packets out for review for swing bed services.

PROCEDURE:

Acute care social worker receives a packet from an outside source for consideration of Swing bed services. Packet is printed off by social worker, and the SNF intake worksheet is placed as the first sheet. Each of the team members (Nursing Supervisor, pharmacy, billing, PT, and physician) review the packet, and then signs off on bottom of worksheet.

COMMITTEE APPROVALS:

P&P: 3/1/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

CREDENTIALING & PRIVILEGING OF TELEMEDICINE SERVICES: TELERADIOLOGY

DEFINITIONS:

For all intents and purposes, the word "patient(s)" refers to all customers receiving health care services in our facilities, including inpatients, outpatients, residents and clients.

Credentialing- Is the process of determining whether an applicant for appointment or reappointment to the Telemedicine Staff is qualified for membership and the specific clinical privileges based on established professional criteria.

Distant Site - the site where the physician providing the mental health service is located at the time the service is provided via audio/video telecommunications.

Presenter - a health care professional that is at the originating site with the patient and at the start of the telemedicine visit, presents the patient to the physician at the distant site.

Telemedicine - the practice of health care delivery, diagnosis, consultation and treatment and the transfer of medical data through interactive audio, video and data communications that occur in the real-time or near real-time and in the physical presence of the patient.

Diagnostic Teleradiology – Includes the reading and interpretation of any diagnostic imaging study that can be sent over a telemedicine link, including but not limited to the following: Computed tomography (CT) Scans, Ultrasound and Plain films.

The following shall not be considered telemedicine:

1. Telephone conversation (including text messaging)
2. Electronic mail message
3. Facsimile (fax)

POLICY:

It is the policy of Mayers Memorial Hospital District (MMHD) to promote quality patient care by exercising due care in awarding practitioners of the telemedicine staff membership with clinical privileges. MMHD will utilize the credentialing information provided by the contracted telemedicine service to make privileging decisions.

Credentialing & Privileging:
Physicians will be granted privileges through MMHD's Imaging department. As a Joint Commission accredited organization, the contracted teleradiology service has credentialed each radiologist performing interpretation services on behalf of MMHD. The MMHD privileges granted to each teleradiologist are for diagnostic teleradiology. As part of its credentialing process, the contracted teleradiology service has verified that each teleradiologist providing interpretation services to MMHD has the appropriate medical training, certification and other credentials necessary to provide such services.

1) Contracted teleradiology service warrants and ensures the following for each teleradiologist:
   a) Duly licensed and qualified and in good standing to practice medicine in the state of California;
   b) Is board certified/board eligible in radiology and shall maintain such certification during the term of the acknowledgement between the contracted teleradiology service and MMHD;
   c) Has and shall maintain active medical staff privileges at the contracted teleradiology service and MMHD;
   d) Renders interpretation services within the scope of the radiologists' respective privileges as granted by the contracted teleradiology service and MMHD.
   e) Is granted privileges in diagnostic teleradiology that includes the reading and interpretation of any diagnostic imaging study that can be sent over a telemedicine link, including, but not limited the following: computed tomography (CT) scans; ultrasound and plain films.
2) MMHD Reliance on contracted teleradiology service credentialing & issuance of privileges – Based on the above representations and assurances of the contracted teleradiology service and that the contracted teleradiology service will notify MMHD of any action taken that constitutes a reportable event to the NPDB as described in 42 U.S.C. § 11133; and pursuant to TJC standard MS 13.01.01, MMHD may rely on the contracted teleradiology service's privileging and credentialing activities.

PROCEDURE:

Initial Appointment:

1) The contracted teleradiology service will provide Medical Staff at MMHD at least 5 business days prior to the addition of a new teleradiologist:
   a) A teleradiology credentialing profile consisting of:
      - State license
      - DEA
      - Certificate of Insurance
      - ABR Certificate
      - Medical Diploma
      - Post Graduate Certificates
      - Hospital Affiliation List

- Continuing Medical Education (CME) transcript
- Current list of the providers privileges
- OPPE
- Malpractice Summary (if applicable)
- Disciplinary Explanation (if applicable)

2) Application Processing: Upon receipt of the above documentation at Medical Staff Administration, the applicant's documents will be placed into their credentialing file, and the following will be performed:
   a) Database Update: The applicant's information will be added to the Medical Staff Administration database
3) Credentialing Review and Approval Process:
   a) The new teleradiologist will be added to the Credentials Committee agenda and that all primary source verifications have been performed by the contracted teleradiology service per the TJC standards.
   b) The Medical Executive Committee (MEC) shall act upon the credentials Committee's report and recommendations at its next regularly scheduled meeting
   c) The MEC shall forward to the governing body, a recommendation as to medical staff appointment.
   d) The governing body shall act on the recommendation of the Medical Executive Committee no more than 60 days after receipt of the recommendation.
4) Medical Staff Administration shall perform the following:
   a) Query the NPDB for adverse actions
   b) Update database with the new appointment dates, etc.
   c) Incorporate the teleradiology service documentation and supplementary verifications and documentation into the credentialing file
   d) Notify the teleradiology service of the appointment dates.

Reappointment:

1) The contracted teleradiology service reappointment process shall be completed prior to expiration of current privileges and within 2 years of initial appointment date. The renewal approval process by contracted teleradiology service shall follow the same process as that of granting initial privileges. The contracted teleradiology service will verify the following:
   a) Any change in relevant education, training and experience since initial privileging;
   b) Verification of current licensure, including any actions taken against the license;
   c) An updated health statement from the applicant confirming they can perform the service he/she has been providing
   d) Query of the NPDB for adverse privilege actions
   e) Two current peer references;
2) Medical Staff reappointment process:
   a) At least 3 months prior to the expiration of the current staff appointment, a request will be sent to the contracted teleradiology service for an updated profile consisting of:
      - State license

- DEA
- Certificate of Insurance
- ABR Certificate
- Hospital Affiliation List
- Continuing Medical Education (CME) transcript
- Current list of the providers privileges
- OPPE
- Malpractice Summary (if applicable)
- Disciplinary Explanation (if applicable)

b) MMHD peer review cases assigned category III or higher will be taken into account at the time of reappointment and will be available to the Credentials Committee and Medical Executive Committee.

3) Primary Source Verifications:
   a) Primary source queries are completed by the contracted teleradiology service. Any outlying information will be reviewed by the Medial Staff Administration office, and at credentials committee.
   b) In addition, Medical Staff Administration will run primary source queries on NPDB
4) Completed Re-Credentialing Review and Approval Process:
   a) Medical Staff Administration will review any MMHD peer review cases, identified in the previous 24 months and flag for discussion at the next credentials committee.
   b) The Credentials Committee shall review and recommend to the MEC the appointment and requested clinical privileges.
   c) The MEC shall act upon the Credentials Committee's report and recommendations at its next regularly scheduled meeting.
   d) The MEC shall forward to the governing body, a recommendation as to medical staff appointment
   e) The governing body shall act on the recommendation of the MEC no more than 60 days after receipt of the recommendation.
   f) Medical Staff Administration shall perform the following:
      i) Update database with the new appointment dates, etc.
      ii) Incorporate the contracted teleradiology service documentation and supplementary verifications and documentation into the credential file
      iii) Notify the contracted teleradiology service of the appointment dates.

REFERENCES:
TJC MS 13.0101
42CFR 482.12(a)(1) through (a)(9)
482.22(a)(1) through (a)(4)

COMMITTEE APPROVALS:
P&P: 9/13/2018
MEC: 10/24/2018

MAYERS MEMORIAL HOSPITAL DISTRICT

POLICY AND PROCEDURE

TRANSMISSION SECURITY

Synopsis of Policy: ***HIPAA Regulation:*** *164.312(e)(1) Transmission security; Integrity controls; Encryption and decryption; Encryption*

This policy creates the rules which guard against unauthorized access to, or modification of, Electronic Protected Health Information (ePHI) ***that is being transmitted over an electronic communications network*** *("data in motion"). It commits resources to assure that when ePHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.*

The policy details standards of encryption, and under which circumstance it is required and when it is optional.

It specifies control requirements of:

- *Modem use;*
- *WAN access;*
- *Wireless devices;*
- *Perimeter security; and*
- *Firewall and details management and workforce responsibilities to execute the policy.*

DEFINITIONS

- Covered Entity: A health plan or a health care provider who stores or transmits any health information in electronic form in connection with a HIPAA transaction.
- Business Associate Definition: any entity that uses or discloses protected health information (PHI) on behalf of a covered entity (e.g. group health plan, hospital, etc.). Furthermore, it is any person or organization who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

- ePHI: Electronic/Protected health information means individually identifiable health information:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.
  - Paper PHI: Protected Health Information that is not in an electronic format.

PURPOSE:

The intent of this policy is to guard against unauthorized access to, or modification of, ePHI that is being transmitted over an electronic communications networks. When ePHI is transmitted from one point to another, it shall be protected in an encrypted manner.

POLICY:

Encryption:
Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the HIPAA Security Officer.

Encryption Required:

1. No ePHI shall be sent outside Mayers Memorial Hospital District (MMHD) domain unless it is encrypted. This includes all email and email attachments sent over a public internet connection.
2. When accessing a secure network an encryption communication method, such as a VPN, shall be used.

Encryption Optional:

1. When using a point-to-point communication protocol to transmit ePHI, no encryption is required.
2. Dial-up connections directly into secure networks are considered to be secure connections for ePHI and no encryption is required.

If still using Modems:

1. Modems shall never be left connected to personal computers in auto-answer mode.
2. Dialing directly into or out of a desktop computer that is simultaneously connected to a local area network (LAN) or another internal communication network is prohibited.
3. Dial-up access to WAN-connected personal computers at the office is prohibited.

ePHI Transmissions Using Wireless LANs and Devices within [ORGANIZATION] domain:

A) The transmission of ePHI over a wireless network within MMHD's domain is permitted if both of the following conditions are met:
    1. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized; and

2. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network and uses two types of authentication.

B) If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI shall be encrypted before transmission.

Perimeter Security

1. Any external connection to MMHD Wide Area Network (WAN) shall come through the perimeter security's Firewall.
2. If determined safe by the Security Officer, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case-by-case basis with the Security Officer.
4. All workforce members connecting to the WAN shall sign MMHD IT Confidentiality Agreement before connectivity is established.

Firewall Controls to Transmit ePHI Into and Out of [ORGANIZATION]

1. Networks containing systems and applications with ePHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
   A. Limit network access to only authorized workforce members and entities;
   B. Limit network access to only legitimate or established connections (An established connection is return - traffic in response to an application request submitted from within the secure network.); and
   C. Console and other management ports shall be appropriately secured or disabled.
3. The configuration of firewalls used to protect networks containing ePHI-based systems and applications shall be submitted to the Security Officer for review and approval.

Policy Responsibilities:

All workforce members that transmit ePHI outside MMHD WAN are responsible for ensuring the information is safeguarded by using encryption when using the public internet or a wireless device.

PROCEDURES

Each area of MMHD shall submit all new and revised procedures to the Compliance Officers for approval and ongoing evaluation. Any procedures developed by MMHD shall be consistent with MMHD**'s** HIPAA policies and not deviate from MMHD standard.

REFERENCES
HIPAA Regulation:

- 164.312(e)(1) *Transmission security*
- 164.312(e)(1) *Integrity controls*
- 164.312(a)(1) *Encryption and decryption*
- 164.312(a)(1) *Encryption*

COMMITTEE APPROVALS:
HIM/HIPAA: 10/25/2018