

Chief Executive Officer  
Louis Ward, MHA



**Mayers Memorial Hospital District**

**Board of Directors**  
Jeanne Utterback, President  
Beatriz Vasquez, PhD, Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

Board of Directors  
**Regular Meeting Agenda**  
August 25, 2021 at 11:30 am  
Mayers Memorial Hospital District  
Burney Boardroom  
20647 Commerce Way  
Burney, CA 96013  
Zoom Meeting Information

[CLICK HERE TO ENTER](#)

Call In Number: 1-253-215-8782 Meeting ID: 846 5290 2031

**Mission Statement**

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

In observance of the Americans with Disabilities Act, please notify us at 530-336-5511, ext 1264 at least 48 hours in advance of the meeting so that we may provide the agenda in alternative formats or make disability-related modifications and accommodations. The District will make every attempt to accommodate your request.

				<b>Approx. Time Allotted</b>
<b>1</b>	<b>CALL MEETING TO ORDER</b>			
<b>2</b>	<b>2.1 CALL FOR REQUEST FROM THE AUDIENCE - PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS</b>			
		Persons wishing to address the Board are requested to fill out a "Request Form" prior to the beginning of the meeting (forms are available from the Clerk of the Board, 43563 Highway 299 East, Fall River Mills, or in the Boardroom). If you have documents to present for the members of the Board of Directors to review, please provide a minimum of nine copies. When the President announces the public comment period, requestors will be called upon one-at-a time, please stand and give your name and comments. Each speaker is allocated five minutes to speak. Comments should be limited to matters within the jurisdiction of the Board. Pursuant to the Brown Act (Govt. Code section 54950 et seq.) action or Board discussion cannot be taken on open time matters other than to receive the comments and, if deemed necessary, to refer the subject matter to the appropriate department for follow-up and/or to schedule the matter on a subsequent Board Agenda.		
<b>3</b>	<b>APPROVAL OF MINUTES</b>			
	3.1 Regular Meeting – July 28, 2021	<b>Attachment A</b>	<b>Action Item</b>	2 min.
	3.2 Special Meeting – August 11, 2021	<b>Attachment B</b>	<b>Action Item</b>	2 min.
<b>4</b>	<b>DEPARTMENT/QUARTERLY REPORTS/RECOGNITIONS:</b>			
	4.1 Resolution 2021-16 – July Employee of the Month	<b>Attachment C</b>	<b>Action Item</b>	2 min.
	4.2 Mayers Rural Health Clinic Update – Amanda Ponti, Manager	<b>Attachment D</b>	Report	2 min.
	4.3 Director of Skilled Nursing Facility – Shelley Lee	<b>Attachment E</b>	Report	2 min.
	4.4 Hospice Quarterly Report – Mary Ranquist	<b>Attachment F</b>	Report	2 min.
	4.5 Safety 6 Month Update – Val Lakey	<b>Attachment G</b>	Report	2 min.
<b>5</b>	<b>BOARD COMMITTEES</b>			
	<b>5.1 Finance Committee</b>			
	5.1.1 Committee Meeting Report: Chair Hathaway		Report	5 min.
	5.1.2 July 2021 Financial Review, AP, AR and Acceptance of Financials		<b>Action Item</b>	5 min.
	5.1.3 401 K Annual Report		Report	2 min.

5.1.4	Managed Security Services (IT) Agreement/Proposal	<b>Attachment H</b>		
5.2	<b>Strategic Planning Committee</b>			
5.2.1	July 28 <sup>th</sup> Presentation from SP Workshop Attached	<b>Attachment I</b>	Report	2 min.
5.2.2	DRAFT Strategic Plan Update		Discussion	10 min.
5.3	<b>Quality Committee</b>			
5.3.1	August 11 <sup>th</sup> Meeting Report – DRAFT Minutes Attached	<b>Attachment J</b>	Report	5 min.
6	<b>NEW BUSINESS</b>			
6.1			<b>Action Item</b>	2 min.
7	<b>ADMINISTRATIVE REPORTS</b>			
7.1	ED of Community Relations & Business Development – Val Lakey	<b>Attachment K</b>	Report	5 min.
7.2	Chief's Reports – <b><i>Written reports provided. Questions pertaining to written report and verbal report of any new items</i></b>		Reports	
7.2.1	Chief Financial Officer – Travis Lakey		Report	5 min.
7.2.2	Chief Clinical Officer – Keith Earnest	<b>Attachment L</b>	Report	5 min.
7.2.3	Chief Nursing Officer – Candy Vculek		Report	5 min.
7.2.4	Chief Operation Officer – Ryan Harris		Report	5 min.
7.2.5	Chief Executive Officer – Louis Ward		Report	5 min.
8	<b>OTHER INFORMATION/ANNOUNCEMENTS</b>			
8.1	Board Member Message: Points to highlight in message		Discussion	5 min.
9	<b>ANNOUNCEMENT OF CLOSED SESSION</b>			
9.1	<b>Personnel Government Code 54957:</b> CEO Evaluation			Discussion
10	<b>ADJOURNMENT: Next Meeting September 22, 2021</b>			

Posted 8/20/2021

Chief Executive Officer  
Louis Ward, MHA



**Mayers Memorial Hospital District**

**Board of Directors**  
Jeanne Utterback, President  
Beatriz Vasquez, PhD, Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

**Board of Directors  
Regular Meeting  
Minutes**

July 28, 2021 – 10:30 am  
MMHD FR Boardroom

*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:** Jeanne Utterback called the regular meeting to order at 10:35 AM on the above date.

**BOARD MEMBERS PRESENT:**

Jeanne Utterback, President  
Beatriz Vasquez, PhD, Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

**ABSENT:**

**STAFF PRESENT:**

Louis Ward, CEO  
Ryan Harris, COO  
Travis Lakey, CFO  
Keith Earnest, CCO  
Candy Detchon, CNO  
Val Lakey, ED of CR & BD  
Tracy Geisler, MHF Executive Director  
Amanda Ponti, Clinic Manager  
Libby Mee, Director of Human Resources  
Jessica DeCoito, Board Clerk

**2 CALL FOR REQUEST FROM THE AUDIENCE - PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS:** PUBLIC COMMENT TAKEN BY BOARD MEMBER THAT OUR PHONE SYSTEM IS CUMBERSOME. PLEASE NOTE THAT ALL EMERGENCIES SHOULD GO TO 911 AND NOT THROUGH OUR PHONE SYSTEM.

**3 APPROVAL OF MINUTES**

A motion/second carried; Board of Directors accepted the minutes of June 23, 2021. **Vasquez, Hathaway** **Approved by All**

**4 DEPARTMENT/OPERATIONS REPORTS/RECOGNITIONS**

4.1 A motion/second carried; Kathi Valencia was recognized as June Employee of the Month. Resolution 2021-14. Retail Pharmacy Technician – such a great asset to our team. Thankful for her hard work and dedication to our pharmacy and our patients. **Hathaway, Humphry** **Approved by All**

4.2 Mayers Rural Health Clinic Update: Clarifications made on the financial statements for RHC in the financials provided by the Finance Department. Lab interface is up and running with some bugs that we are working through. Thank you to IT and Jack Hathaway with getting the interface set up and running. Plan of Corrections was returned to Amanda on Monday and will have comments returned to them by August 2<sup>nd</sup>. Then a 30-day window to process is given. We only have one finding to address. At this time Dr. Saborido will not be seeing patients at our clinic. A letter from Dr. Saborido will be sent out to each patient he has seen since the opening of the clinic. We are actively searching for a new provider to fill this spot and interviews have already been set up.

4.3 Director of Human Resources: site visit with HR Peers will probably be rescheduled given the current fires in Plumas County. We have been in touch with providing our resources to those healthcare facilities impacted by these wildfires. 67% vaccinated in our employees. We are working on keeping up on the education for our staff and the vaccinations. Discussion about the legality of mandating the COVID vaccine has taken place with legal counsel and the Board Quality Committee. We have discussed policies being set in place to meet a mandate but provide exemptions for certain situations. Recommendation to have staff draft up a plan for incentives, policies and educational outlets for our staff members and our community, understanding that we will potentially see a mandate come down from the state or federal government on being mandated.

4.4	Worker's Comp 6 Month Report: Rate goes up per the payroll going up. BETA initiative – we are 1 of 2 facilities who successfully implemented the ergonomics program.		
4.5	Mayers Healthcare Foundation Quarterly Report: delighted to have Jeanine Ferguson join the team as Volunteer and Event Coordinator. New development of a vacancy on the Board. A committee has been formed and information will be sent out. Open to receiving help with the Golf Tournament organization and coordination. Jeanine is working on getting this ball rolling and will keep you all in mind for volunteering before or the day of.		
<b>5</b>	<b>BOARD COMMITTEES</b>		
5.1	<b>Finance Committee</b>		
5.1.1	<b>Committee Report:</b> Retail Pharmacy inventory is still a struggle but we are working with staff to understand the processes in place now. 340B conversation will take place with MVHC on July 29 <sup>th</sup> . Heard from Dietary Manager, Susan Garcia, on revenues from café sales which has been down with COVID and closure to public. We also heard that our refrigeration and freezer units have had failures 5 times in the locations in the past two months which is approx. \$1200 each time. Units are old and exposed to the elements which has caused bigger issues with functionality.		
5.1.2	<b>June 2021:</b> 58.29 AR Days, AP 1,044,461	<i>Hathaway, Humphry</i>	<i>Approved by All</i>
5.2	<b>Strategic Planning Committee Chair Vasquez</b>		
5.2.1	<b>SP Planning Session:</b> following regular board meeting at 1:00 pm		
5.3	<b>Quality Committee Chair Utterback</b>		
5.3.1	<b>Committee Meeting Report</b> – very similar discussion to what we had here today regarding the legality of mandating the vaccine. Health Information Management: transferring of patient records from clinics back to our ER doctors and nurses. Our clinic is currently not experiencing any issues getting patient records transferred from other facilities. It's not uncommon for a patient being seen in the ER setting having some issues with getting records from primary care physician because: 1. It's after hours on primary care facility 2. Our previous situation was our ER physician was also the primary care physician at the clinic and transferring of records was much easier.		
<b>6</b>	<b>NEW BUSINESS</b>		
6.1	Policy and Procedure Summary 6-30-2021	<i>Vasquez, Hathaway</i>	<i>Approved by All</i>
6.2	Policies & Procedures: <ol style="list-style-type: none"> <li>1. Air Exchange in Operating Room</li> <li>2. Bladder Scan Policy Using the PBS Bladder Scanner</li> <li>3. Disbursement of Funds</li> <li>4. Scope of Services MMHD</li> </ol>	<i>Guyn, Hathaway</i>	<i>Approved by All</i>
<b>7</b>	<b>ADMINISTRATIVE REPORTS</b>		
7.1	<b>ED of Community Relations &amp; Business Development:</b> Great job on the commercial. Commended for all the efforts with the CODES and Emergency Preparedness materials and training occurring.		
7.2	<b>Chief's Reports</b>		
7.2.1	<b>CFO:</b> Great collections month in June. Auditors are here on August 16 <sup>th</sup> .		
7.2.2	<b>CCO:</b> Vaccination clinic has hit some challenges with employees in other industries not wanting to receive the vaccine. 340B – conversation will take place tomorrow 7/29 with MVHC and MMHD CEO and CFO. Physical Therapy has worked out a situation to house the DME equipment and send out to patient's home with the required equipment rather than try and work out the delivery schedule.		
7.2.3	<b>CNO:</b> Lab hood should be done very soon. And our manager is doing very well in his new role. Radiology continues to have staffing issues. Internet has been fixed and issue is resolved. Acute Care Boot Camp worked out really well with educating the staff.		
7.2.4	<b>COO:</b> Daycare: plans need approval before we can begin work. And then licensing will start all over once building/remodeling has been completed. OSHPD is changing to Department of Healthcare Access and Information - will take time to review their processes. Water Tank update: too many contaminants in our water		

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](http://www.mayersmemorial.com).

which could be coming from CSD. Working on where the contaminants are coming from which is affecting our substantial completion. Security Audit: didn't pass certain phases of the audit but helped us identify what the methods of educating staff will be. Dietary: staffing is down. Big thanks to staff and manager for picking up the extra shifts.

- 7.2.5 **CEO:** We've been spending a lot of time researching potential providers. The CA mandate has been a hot topic and we are continuing that discussion with our team. Housing continues to be an area of concern that we continue to work on. EMR (electronic medical records) – met with the OCHIN team and continue to have discussions about moving into EPIC here for the hospital, in addition to the clinic.

---

**8 OTHER INFORMATION/ANNOUNCEMENTS**

---

- 8.1 Board Member Message: Employee of the month, Ergonomics Award, reminder of the COVID vaccinations, MHF Golf Tournament.

---

**9 ANNOUNCEMENT OF CLOSED SESSION: 12:45 PM**

---

9.1 **Medical Staff Credentials Government Code 54962**

**AHP APPOINTMENT**

1. Vadim Smirnov, CRNA
2. Sharon Hanson, NP – Family Medicine (Outpatient Only)

**AHP REAPPOINTMENT**

1. Marchita Masters, PsyD – Telemedicine
2. Adam Gardizi, CRNA

**MEDICAL STAFF APPOINTMENT**

1. Jesus Pereyra, MD – Radiology, Telemedicine
2. Denis Primakov, MD – Radiology, Telemedicine
3. Cierra McNair, MD – Radiology, Telemedicine
4. Larry Givens, MD – Radiology, Telemedicine
5. Barry Shibuya, MD – Rheumatology, Telemedicine
6. Pamela Ikuta, DO – Emergency Med
7. Richard Leach, MD – Emergency Med
8. Chuck Colas, DO – Family Medicine (Consulting Priv.)
9. Tawana Nix, DO – Family Medicine (Consulting Priv.)
10. Dan Dahle, MD – Family Medicine (Consulting Priv.)
11. Sheela C. Toprani, MD – Neurology, Telemedicine
12. Elizabeth Ekpo, MD – Neurology, Telemedicine
13. Jodi Nagelberg, MD – Endocrinology, Telemedicine

**MEDICAL STAFF REAPPOINTMENT**

1. Aaron Babb, MD – Family Med (Consulting Priv.)

- 
- 9.2 **Personnel Government Code 54957: CEO Evaluation:** will continue discussion into next month's Discussion  
CLOSED Session.

- 
- 9.3 **Pending Litigation Government Code 54596.9: Mediation Update:** settlement has been reached. Information
- 

**10 ADJOURNMENT: 1:30 pm**

Next Regular Meeting: August 25, 2021 – Burney Boardroom

*Approved by  
All*

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](http://www.mayersmemorial.com).

Chief Executive Officer  
Louis Ward, MHA



**Mayers Memorial Hospital District**

**Board of Directors**  
Jeanne Utterback, President  
Beatriz Vasquez, PhD, Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

Board of Directors  
**Special Meeting**  
**Minutes**  
August 11, 2021 – 12:45 pm  
Teleconference Only

*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:** Jeanne Utterback called the special meeting to order at 12:45 PM on the above date.

---

**BOARD MEMBERS PRESENT:**

Jeanne Utterback, President  
Beatriz Vasquez, PhD, Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

**STAFF PRESENT:**

Travis Lakey, CFO  
Jessica DeCoito, Board Clerk

**ABSENT:**

---

**2 CALL FOR REQUEST FROM THE AUDIENCE - PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS: NONE**

---

**3 Resolution 2021-15:** Hospital Expansion Settlement Agreement: motion moved, **Guyn, Hathaway** Hathaway – Y  
seconded and carried to approve the Resolution to accept and approve the Guyn – Y  
settlement. Humphry – Y  
Utterback – Y  
Vasquez - Y

---

**4 OTHER INFORMATION/ANNOUNCEMENTS**

---

**6 ADJOURNMENT: 12:50 pm**

---

Next Regular Meeting: August 25, 2021

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



**Mayers Memorial Hospital District**  
*Always Caring. Always Here.*

**RESOLUTION NO. 2021-16**

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

**Samantha Clark**

**As July 2021 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, Samantha Clark is hereby named Mayers Memorial Hospital District Employee of the Month for July 2021; and

**DULY PASSED AND ADOPTED** this 25th day of August 2021 by the Board of Trustees of Mayers Memorial Hospital District by the following vote:

AYES:  
NOES:  
ABSENT:  
ABSTAIN:

---

Jeanne Utterback, President  
Board of Trustees, Mayers Memorial Hospital District

ATTEST:

---

Valerie Lakey  
Acting Clerk of the Board of Directors

Chief Executive Officer  
Louis Ward, MHA



Mayers Memorial Hospital District

Board of Directors  
Jeanne Utterback, President  
Beatriz Vasquez, Ph.D., Vice President  
Tom Guyn, M.D., Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

## **Board Meeting**

Wednesday August 25, 2021

### **Mayers Rural Health Center Report – Amanda Ponti, Clinic Manager**

#### **Survey Update**

On 6/18/2021, we received our Clinical Laboratory Improvement Amendments (CLIA) certificate and began running point of care lab tests in the clinic. This has been a long awaited process that we are glad is complete.

On 7/15/2021, the clinic staff participated in the unannounced Compliance Team survey. The staff handled the survey well and we were given great remarks from the surveyor. The Compliance Team has 10 business days to report their findings that need a plan of correction. In the exit portion of the survey only two findings were reported which included an expired medication in the emergency box (which was removed upon finding), and the need for a lid on the transport bin for sterilization instruments. Both of these items have been corrected.

The completion of this survey means we can finalize our Medicare enrollment, apply for our Provider Transaction Access Number (PTAN), complete our Partnership Health Plan (PHP) contract and apply for our visit rates.

#### **Electronic Medical Record Interface Updates**

Work on the laboratory interface between Mayers Hospital Lab and the Clinic was put into production 7/16. We are still working out the process modifications that are needed now that this is live, however it is very exciting to have provider ordered testing go directly to our lab and results return and file into EPIC.

The radiology interface is in the testing phase and will likely be live in the next few weeks.

The IT department has put a significant amount of work into these projects. I am grateful to have such reliable and engaged support from that entire team.

#### **Outstanding Program Registration**

Applications are still in process for the following programs to extend services offered at the clinic:

Child Health and Disability Prevention (CHDP) – awaiting VFC number

Family Planning (FPACT) – still collecting information

Vaccinations for Children (VFC) – waiting on help from Keith on application



## Statistics

The clinic has currently completed 1210 visits serving 546 patient as of 7/16/21 with 169 productive provider days.

Average patients per day for the last 30 days by provider are currently: Corr 11, Haedrich 6.25, Dr. McKenzie 13, Dr. Saborido 7, and Syverson 5.

The clinic has processed 547 outgoing referrals to the following services:

AUDIOLOGY	2	OPHTHALMOLOGY	1
BARIATRIC SURGERY	1	OPTOMETRY	2
BONE DENSITY TESTING	7	ORTHOPEDIC SURGERY	5
CARDIAC REHAB	2	ORTHOPEDICS	7
CARDIOLOGY	20	PAIN MANAGEMENT	4
CAROTID ULTRASOUND	1	PHY MED/REHAB	3
CHIROPRACTIC	2	PHYSIATRY	1
COLONOSCOPY	2	PHYSICAL THERAPY	49
CT	38	PLASTIC SURGERY	2
DERMATOLOGY	3	PODIATRY	2
Dexa Scan	14	PROSTHETICS	1
DIABETIC RETINAL EXAM	7	PSYCHIATRIST/PSYCHOLOGIST	2
EAR, NOSE AND THROAT	7	PSYCHOLOGY	3
ECHO	6	PULMONARY FUNCTION TEST	2
ELECTROMYOGRAPHY	1	PULMONOLOGY	3
GASTROENTEROLOGY	14	REFERRAL FOR WOUND CARE	1
GENERAL SURGERY	28	RHEUMATOLOGY	3
GYNECOLOGY	3	SLEEP STUDY	2
HEMATOLOGY	1	SPINE CLINIC	7
HOLTER MONITOR	3	SURGICAL CONSULT	1
HOME SLEEP STUDY	1	U/S OF KIDNEY/BLADDER	1
MAMMOGRAM	46	ULTRASOUND	56
MRI	42	UPPER GI	3
NEPHROLOGY	2	UROLOGY	7
NERVE CONDUCTION STUDY	2	US CAROTID DUPLEX COMPLETE BILATERAL	1
NEUROLOGY	5	VASCULAR SURGERY	1
NEUROSURGERY	3	X-RAY	113
OB/GYN	1		

Additionally the clinic has ordered 2,447 lab tests

# SNF BOARD REPORT

AUGUST 16, 2021

- Current Census is 78. Fall River has 5 female and 2 male beds available and are expecting 2 possible admits. Burney has 1 male bed left in the general population and the memory care unit is full.
- Fall River is currently being tested for a direct exposure from staff. No positive test for Covid from residents. Burney has also had an indirect exposure from staff.
- Multiple staff members getting vaccinated since the incentive came out.
- The latest changes in regulation now require us to test any unvaccinated visitor. We are using a rapid test that takes 15 minutes. All Family, POA or Conservator were sent an email and text to notify them of the new requirements for visitation. We are keeping all proof of vaccination of for each residents visitors' to reference at each visit.
- We have established a new Team to work on reducing the use of Anti-Psychotic medications. Education will be provided for staff on managing resident behaviors without the use of medication and improving documentation for the use of Psychotropic meds.
- We have interviewed and hired 2 LVNS AND 2 CNAS.
- We continue to work with CDPH on our own CNA class.

# HOSPICE BOARD REPORT

07/27/2021

## Statistics:

Patients served: (01/01/2021—07/26/2021) 32

Average Daily Census (04/01/2021—06/30/2021) 6.51 patients

Yearly Average Length of Stay-- 33.78 days

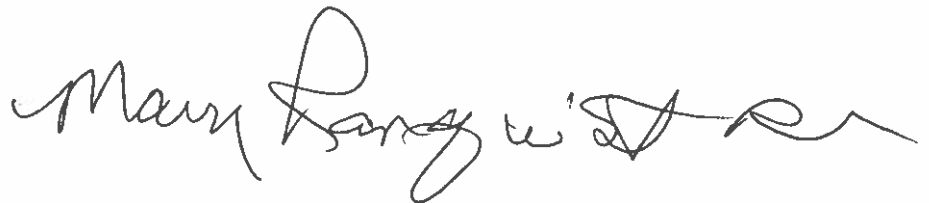
## Hospice News:

We have currently serviced 32 patients this year. This is very close to an "End of The Year" Census Total. We have been busy with patients in all three counties that we service. Our referrals are coming in steadily. July has been a busy month with 5 admissions and 3 deaths.

The Hospice Car was involved in an accident over the last month. The car was parked in its parking place and was hit by a reckless driver. Unfortunately, the car is not able to be fixed. The hospice staff is looking forward to getting a replacement as soon as possible.

The Annual Hospice Show & Shine Car Show was held on July 18<sup>th</sup>. The Nor Cal Road Gypsies sponsored the event. It was a success. The Show was well attended. The Raffle was successful. People enjoyed the food, cars, and music. We have already started plans to add a Coffee and Doughnuts Table which will be supplied by the Hospice Staff and Volunteers.

Lindsey Crum, Hospice LVN has been accepted into the RN program at Carrington College and will begin her studies on Aug. 6<sup>th</sup>. She will be missed greatly by our team. A position has been posted to our internal and external employment opportunities. Congratulations to Lindsey Crum.

A handwritten signature in black ink, appearing to read "Mary Lang". The signature is written in a cursive style with a large initial "M" and a long, sweeping tail.



**Mayers Memorial Hospital District**  
*Always Caring. Always Here.*

### **Safety/ Emergency Preparedness Quarterly Report**

August 25, 2021 Regular Board Meeting

Presented by: Valerie Lakey

The Safety and Emergency Preparedness Department is an important part of our operations at MMHD. We have been emphasizing the importance of “knowing what you need to know before you need to know it.”

The Ergonomics Program is fully completed. This program will ensure staff and patient safety and outline processes, education and training. The Ergonomic program will impact patients in a positive way. Training for safe patient handling and proper work place safety is essential to maintain a capable and safe workforce.

Through the ergonomic program, staff will have more access to resources, education and training. The program maintains a goal of providing safe work environments. Routine evaluations of workstations, processes and equipment will help identify any issues before they become a challenge. Wellness Coordinator, Dana Hauge has been instrumental in these programs. Dana completed Ergonomic certification and is doing a great job building this program.

The Safety committee meets monthly and has representation from departments. We have added Cybersecurity to our regular monthly topics.

We have almost completed a new resource binder that aligns Emergency Preparedness survey items with our back-up and implementation of the required processes.

The Safety and Emergency Preparedness Department has been focused on preparing staff for emergency situations. In highlighting the most significant things that are going well:

- Monthly Code Training, Education and Drills
- Updated Employee Resources on the Intranet and MyEOP App
- In-person department trainings

The monthly focus on a new EMERGENCY CODE is a direct result of a Plan of Corrections. Working with the Director of Quality, we established a calendar for CODE training and education. Each month we focus on a new code. There is education provided to staff, quizzes and a drill. An After Action Review (AAR) is completed for each month’s code to determine what capabilities we need to work on.

CYGILANT RESPONSE TO RFP

# Mayers Memorial Hospital District

Managed Security Services/Security Operations Center (SOC) Provider  
Technical Proposal

**Submitted by:**

Cygilant  
2400 District Avenue  
Burlington, MA 01803  
POC: Cooper Mooney  
cmooney@cygilant.com  
617.337.4839

**Submitted August 6th, 2021**



**CYGILANT®**

## Table of Contents

<b>1. <i>Introductory Letter</i></b> .....	<b>3</b>
<b>2. <i>Cygilant Cost Proposal</i></b> .....	<b>4</b>
<b>3. <i>Estimated Implementation Timeline</i></b> .....	<b>5</b>
<b>4. <i>Accurately Completed Questionnaire (Attachment A)</i></b> .....	<b>7</b>
<b>a. <i>Company</i></b> .....	<b>7</b>
<b>b. <i>Compliance</i></b> .....	<b>10</b>
<b>c. <i>Technology</i></b> .....	<b>12</b>
<b>d. <i>MDR</i></b> .....	<b>25</b>
<b>e. <i>Incident Analysis and Response</i></b> .....	<b>28</b>
<b>f. <i>Metrics, Reporting and Dashboard</i></b> .....	<b>34</b>
<b>g. <i>Data Management</i></b> .....	<b>35</b>
<b>h. <i>Pricing</i></b> .....	<b>36</b>
<b>i. <i>Client Satisfaction</i></b> .....	<b>36</b>
<b>5. <i>Cygilant Security-as-a-Service Technical Explanation</i></b> .....	<b>39</b>
<b>6. <i>References</i></b> .....	<b>46</b>
<b>7. <i>Additional Information</i></b> .....	<b>47</b>
<b>a. <i>Sample Monthly SOC Report</i></b> .....	<b>47-53</b>



## 1. Introductory Letter

Subject: Mayers Memorial Hospital District Request for Proposal (RFP) 2021

Dear Ryan,

Cygilant is very pleased and excited to submit our response to the Mayers Memorial Hospital District Managed Security Services Provider/SOC RFP.

Cybersecurity is hard work. Resource constraints – not enough time or limited resources – and ever-increasing threats coupled with compliance requirements are leaving many businesses at a disadvantage and causing stress. Cygilant exists to help you. We partner to extend your team with cybersecurity-as-a-service that overcomes resource constraints, reduces threats and helps achieves compliance. Our main goal is to help you reduce the stress of cybersecurity.

We are excited to work with Mayers Memorial Hospital District who has taken a major initiative to complete, not only 24x7x365 network coverage and visibility, but map towards and improve their security objectives. With this initiative, a partnership with Cygilant can transform the Hospital District from a potential victim to a proactive, cyber stronghold. With Cygilant, we demand excellence, and we will protect Mayers Memorial Hospital District 24x7x365 to ensure you can rest easy knowing you are secure. We are more than a cybersecurity vendor – we are a partnership, and we look forward to working with the District in the near future.

If you need any additional information, please reach out to me at [cmooney@cygilant.com](mailto:cmooney@cygilant.com).

All the best,

Cooper Mooney

Senior Account Executive – West Coast at Cygilant

(203) 695-4918 – Cell

<https://www.linkedin.com/in/cooper-mooney-bb151a107/>

## 2. Cygilant Cost Proposal – Mayers Memorial Hospital District RFP

	1 Yr Agreement
Cygilant 24x7 SOCVue Security-as-a-Service	Cost Per/Year
SOCVue Security Monitoring Service – AlienVault USM Anywhere 1.5 TB/Month, 15 Days Hot Storage and Cold Archival Storage	\$76,800
SOCVue Endpoint Management Service – SentinelOne Control 370 Endpoints (135 Servers & 235 Workstations)	\$26,418
SOCVue Qualys Vulnerability Management Service – Qualys Vulnerability Scanner and 500 IPs (external and internal)	\$18,690
<b>Cygilant 24x7 SOCVue Security-as-a-Service</b>	<b>\$119,652.60</b>

This price is the 1-year annual agreement for Cygilant’s 24x7 SOCVue Security-as-a-Service covering Tasks: 1.1 24x7 SOCVue Security & Threat Monitoring, 1.2 Endpoint Management (Detection + Response), and 1.3 Unlimited Vulnerability Management. This price also includes everything discussed in the attached RFP, with no additional costs involved.

**Cygilant 24x7 SOCVue Security & Threat Monitoring** – This is covered by Cygilant’s SOCVue Security Monitoring service as described in the RFP and Cygilant’s Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to AlienVault USM Anywhere SIEM, which includes 1.5 TB/Month of data consumption, 15 Days Hot Storage of Log Data, Cold Archival Storage of Log Data for the entire duration of the agreement. The installation, configuration, and management of the AlienVault USM Anywhere SIEM is done by Cygilant’s SOC team and the Cybersecurity Advisor, included in the price of the service. The 1.5 TB/Month of data consumption includes every device listed in the Hospital District’s RFP. This is included in Cygilant’s cost proposal above.

**Cygilant Endpoint Management (Detection + Response)** – This is covered by Cygilant’s Endpoint Management service as described in the RFP and Cygilant’s Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to SentinelOne Control, which includes x endpoint, for the Hospital District’s x servers and x workstations. The installation, configuration, and management of the SentinelOne software is done by Cygilant’s SOC team and the Cybersecurity Advisor, included in the price above.

**Cygilant Unlimited Vulnerability Management** – This is covered by Cygilant’s Endpoint Management service as described in the RFP and Cygilant’s Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to Qualys’ vulnerability scanner, which includes x IPs (both external and internal) for unlimited scanning. The installation, configuration and management of the Qualys Vulnerability Scanner is done by Cygilant’s Cybersecurity Advisor, included in the price above.

Cygilant offers a discounted bundle percentage of 5% for its services, which is included in the proposed cost proposal.

Cygilant offers three-year contract agreements that are additional cost-savings to the Hospital District.



### 3. Estimated Implementation Timeline

The following contains our anticipated project schedule for Mayer Memorial Hospital services:

Activity	Anticipated Timeline in Calendar Days
Complete onboarding	6-8 weeks
Establish change control procedures	
Deploy all required tools and appliances	10-15 days
Train staff in use of all services	No formal training provided
Integrate with and ingest content from existing tools	10-15 days
Required project meetings	Monthly meetings with the Hospital's Cybersecurity Advisor

Activity	Anticipated Timeline
Define success criteria for solution and deployment	Within three Days of Signing Agreement
Build your tailored installation and deployment plan	First week of Service
Install sensor	Partners schedule
Import Nodes or IPs	Five days after install
Performance baselining	Within the first four to six weeks of Service
SOCVue Walkthrough (Review Incidents, Scan Results, Patches and Reporting)	Within the first month of Service
Alert and report customization	Within the second month of Service
Monthly meeting and review with Dedicated Cybersecurity Advisor	Every month of service

The Cygilant onboarding process is described in more detail below and will be performed in three stages:

#### 1. Service Orientation Call

Your Cygilant Account Executive Cooper Mooney will contact you to schedule a Service Orientation Call with your Cygilant Cybersecurity Advisor. The goals of the call will be:

- Introduce the Hospital to the SOCVue Security Monitoring service People, Processes, and Technology
- Identify points of contact
- Define requirements for toolset deployment
- Identify devices on which to monitor

- Provide connectivity requirements for toolset communication

## **2. Installation Call**

After your Service Orientation Call has been performed, you will be contacted to schedule the installation of security monitoring solution. The goals of the installation call will be:

- Install the AlienVault USM Anywhere SIEM solution SentinelOne, and Qualys tool (will need multiple calls, if necessary)
- Test and validate toolset connectivity
- Perform a discovery scan to detect nodes on the network (Qualys)
- Integrate nodes to be monitored (AlienVault)
- Transition to service deployment

## **3. Service Deployment**

Further deployment actions will be performed by your Cybersecurity Advisor and the Cygilant Security Operations Center. The subsequent steps will include:

- Review the status of the onboarding project plan
- Validate contacts to receive notifications
- Set up access to the SOCVue platform
- Discuss reporting needs
- Conduct internal operation readiness review
- Commence with security monitoring deliverables as outlined in Section 4: Service Features

## 4. Accurately Completed Questionnaire (Attachment A)

### 4.a Company

#### 1. How long has your company been in business?

Cygilant has been in business for 20 years, previously as EiQ Networks, Inc. (2001-2017). Cygilant specializes in 24x7 SIEM and threat monitoring and created one of the first Top 5 SIEM technologies, its legacy solution SecureVue, which is still used in the Department of Defense and U.S. Government. Led by a seasoned team of cybersecurity executives and technologists, Cygilant has over 20 years of cybersecurity experience and over 7 years managing a Global Security Operations Center. Cygilant combines security expertise with its best of breed SIEM technology and cybersecurity dashboard, the SOCVue Platform.

#### 2. How many Security Operation Centers do you maintain? Where are they located?

Cygilant operates a 24x7 global Security Operation Center (SOC) located in Belfast, Northern Ireland.

#### 3. How many total employees do you have?

Cygilant currently has 65 employees and is actively hiring.

#### 4. How many of these employees are part of your SOC(s)?

Cygilant has over 35 security professionals in SOC & Security Services, backed up by about 20 engineers in Development, Product Support, DevOps, and Infrastructure Support roles. Over two-thirds of Cygilant staff are exclusively engaged in delivering managed security & SOC services.

#### 5. How long have you offered MSSP/SOC services to your clients?

Cygilant has offered MSSP services since 2001 (formerly EiQ Networks). Cygilant has offered SOC services since 2014.

#### 6. Are clients homed out of a specific monitoring center or is activity shared across all your centers?

There is one centralized 24x7x365 SOC, located in Belfast, Northern Ireland, that monitors the Hospital's complete environment. Cygilant's SOC processes allow for scalable, repeatable, and effective operations. Cygilant's SOC Director, Dr. Ben Harrison, has created a complex, comprehensive alerting system that analyzes numerous factors to determine alert severity. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious

activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

Furthermore, as part of the SOC monitoring activity, you will be assigned a Cybersecurity Advisor. The Cybersecurity Advisor is a one-on-one point of contact that is assigned directly to the Hospital's IT team, to utilize as a true cybersecurity resource. The goal of this Advisor is to understand Mayer Memorial Hospital's security objectives and work to meet them. To do so, the Cygilant Cybersecurity Advisor will schedule monthly one-on-one review sessions to review open tickets and incidents, analyze alert trends, configure and maintain the SIEM technology, discuss needed improvements for SOC monitoring, define and finetune reporting needs and future deployment plans, and schedule follow-up calls as needed. During these meetings, the Cybersecurity Advisor can answer any questions the Hospital may have about how to improve and mature their cybersecurity posture.

**7. Approximately how many clients do you have fully implemented in your MSSP/SOC offering?**

Cygilant has over 150 partners fully implemented in our MSSP/SOC offering.

**8. How many of these clients are in healthcare?**

~25 percent of Cygilant clients are in healthcare.

**9. Are you willing to demonstrate your services in a proof of concept implementation?**

Yes, Cygilant encourages a complimentary proof of concept for Mayer Memorial Hospital District.

**10. What is your client retention rate?**

Cygilant's client retention rate is over 90%, with most customers purchasing additional services over the duration of the partnership.

**11. Please describe what you feel differentiates your offering from your competitors.**

Cygilant's Security Monitoring service exists to help Mayer Memorial Hospital proactively identify, respond to, and remediate security threats in their environment. With over 15 years of cybersecurity experience and over 7 years in managing a Global Security Operations Center (SOC), our cybersecurity experts guarantee that if the Hospital chooses Cygilant, they will build, mature, and grow their proactive cybersecurity program. Cygilant has achieved this for our clients in the past by combining our people, process, and technology.

Trust in your Security-as-a-Service (SaaS) provider and their personnel is paramount. In May 2020, Cygilant opened a new Global SOC in Belfast, Northern Ireland, a known cybersecurity hub. Cygilant's SOC operates four tiers of human support on a 24x7 basis. Cygilant

tapped into Belfast's cyber skill pool to staff its SOC with team members holding master's and Doctor of Philosophy (PhD) degrees in cybersecurity and who come from SOC, Network Operating Center (NOC), software engineering, and information technology (IT) backgrounds. Cygilant's SOC team members hold certifications such as CompTIA Security Plus, CEH (Certified Ethical Hacker), Global Information Assurance Certification (GIAC), Cisco, and SANS. The Hospital will have direct access to these experts via phone/email and who will work one-on-one with them as an extension of their team and aid with any threats.

A tried and proven process is also a major component in selecting a SaaS partner. Cygilant's SOC processes allow for scalable, repeatable, and effective operations. Cygilant's SOC Director, Dr. Ben Harrison, has created a complex, comprehensive alerting system that analyzes numerous factors to determine alert severity. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. We want to give you the best actionable alerting in the industry – and we will do so. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

To further this point, being fully secure on a 24x7 basis goes further than just managing your endpoints. A SOC needs visibility into a variety of data sources, not just endpoint events. A well-rounded security monitoring program includes network traffic analysis, security device events (firewall, gateway, etc.), endpoint data, and cloud sources like Office 365 login activity. By combining all this data with a modern SIEM, Cygilant has more information not only for threat detection, but also for tracing the threat across your environment after a suspicious incident occurs. Therefore, we have implemented proven processes that are both entirely customizable to your security needs and customer-centric so that the Hospital can know they are secure and get the most out of your cybersecurity program with Cygilant being your Security-as-a-Service partner.

A third component of choosing a SaaS provider is technology. Cygilant will help Mayer Memorial navigate the messy cybersecurity market by partnering with and providing best-of-breed technologies like AT&T Cybersecurity, SentinelOne, Qualys, etc. All our technologies are Gartner certified and Fortune 500 tried and proven technology, as compared to the other options in the market. In addition to the partnerships we have created, Cygilant has also created and developed its own proprietary technology, our SOCVue Platform. SOCVue simplifies and consolidates multiple streams of security data to help detect and respond to threats faster and effortlessly collaborate. Also, the Hospital will have a centralized platform to see all of the real-time SOC incident response and compliance activities to provide full network visibility. The goal of SOCVue is to make your environment easier to manage, eliminating the need to engage multiple vendors or technologies. Cygilant will manage all that best-of-breed technology for the Hospital and ease deployment, management, and response through our innovative SOCVue platform.

Cygilant is the most affordable boutique Cybersecurity-as-a-service for all-sized organizations and is a true partner in cybersecurity. We want to see you and your team succeed and grow your cybersecurity program as much as you do. That is why we combine our security experts with best of breed technology and a cybersecurity dashboard in a repeatable process-driven service. We want to give you access to everyone at Cygilant, from the Director of our SOC Operations to our CEO – because we value your security objectives and want to ensure we help you achieve them. In partnering with us, not only will you get a boutique, enterprise-level Security-as-a-Service, but you will get the best customer security value in the industry because we put Customer Security Value at the center of our services, where it belongs.

**12. Do you have a dedicated internal threat team? How will you notify MMHD of an internal threat to your environment?**

Yes, Cygilant has an internal threat team that is constantly evaluating and researching known or unexpected threats.

Dependent on the severity of the threat, a Cygilant SOC member will either call your phone directly or ensure we notify you of and remediate the threat. If the threat is less critical, your Cybersecurity Advisor will reach out to you via email with information and a Threat Advisory that details the severity of the threat, its impact on business, actionable remediation guidance, etc.

**13. Please provide any industry certifications your MSSP/SOC hold, such as SOC, ISO, etc.**

Cygilant's SOC team members hold certifications such as CompTIA Security Plus, CEH (Certified Ethical Hacker), Global Information Assurance Certification (GIAC), Cisco, and SANS.

Cygilant holds SOC2 and PCI certification. We are actively working on translating our compliance from SOC2 into parallel ISO 27001 certification.

## **4.b Compliance**

**14. Is your solution able to assist us in identifying systems that store, transmit(send/receive), and access ePHI?**

Cygilant will use the Qualys network scanner to discover systems on your network. You Cygilant Cybersecurity Advisor will work with you to identify which of these systems process ePHI and can create a separate asset inventory group for tracking these systems.

**15. How do you anticipate assisting us in protecting and monitoring access to PHI?**

Cygilant will deploy Qualys vulnerability scanning to detect weaknesses in ePHI systems that could be exploited by attackers. Cygilant will also deploy SentinelOne agents on your servers, workstations, and laptops to detect and block malware. The SentinelOne agent will also use advanced machine learning to detect anomalous behavior on the endpoint that might indicate that someone is trying to gain unauthorized access. Lastly, Cygilant will deploy the AlienVault USM Anywhere solution to collect audit logs and alerts from your network infrastructure. These logs will be monitored by the Cygilant SOC around the clock to identify potential security incidents, which could include outside attacks or misuse by insiders.

**16. How do you intend to secure logs or other telemetry data containing PHI? How long will they be stored?**

Logs and other data collected by Cygilant is encrypted in transit to our systems and encrypted at rest in the products that process and store the information. Logs collected by Cygilant typically contain data like IP addresses, usernames, domains, and file hashes, and do not typically contain any health records. Logs will be stored in “cold storage” in the AlienVault solution for the duration of the contract unless you request it to be purged sooner.

**17. Are you willing to engage in a BAA? Please send a copy.**

Yes, we have engaged in a BAA with other clients and would be willing to do so. If the District would like us to sign a BAA, please send it over for our review and consideration.

**18. Do you use sub-processors to support your environment? If yes, how do you ensure the sub-processors operate securely and effectively?**

Cygilant uses several sub-processors including Amazon Web Services, Zendesk, and the products named above. Cygilant sub-processors are SOC 2 compliant and regularly recertified by third-party auditors. Cygilant reviews sub-processor security controls to ensure Cygilant customer data is being protected by the highest industry standards.

**19. Have you suffered a breach, either from an internal or external actor, in any of the preceding 60 months? Please describe and indicate what was learned from this event?**

Cygilant experienced a cybersecurity event in August 2020. The Cygilant Security Operations Center (SOC) discovered a security threat and immediately reported it for investigation. Cygilant was decommissioning a system housing legacy software when an unknown actor gained access to the environment. The system since has been decommissioned. Cygilant engaged a third-party forensic investigation firm to assist in further understanding the nature and scope of the event. Cygilant also conducted a full review of its cybersecurity policies, procedures, processes, and security measures to ensure that they remain appropriate. Cygilant segregates customer transactional data from other company data housed within its environment. This security measure prevented customer transactional data from being impacted by the event. Cygilant hopes this summary addresses any questions you might have about the now-resolved event. Cygilant remains a trusted advisor and partner in delivering premium and uncompromised Cyber Security as a Service. However, should you have additional questions, please do not hesitate to contact Christina Lattuca at [CLattuca@cygilant.com](mailto:CLattuca@cygilant.com) or (617) 337-4802.

**20. Has a customer ever been breached due another customer’s breach?**

No.

## 4.c Technology

### 21. Describe your implementation and tuning process for a new customer. How long does this usually take?

The following contains our anticipated project schedule for Mayer Memorial Hospital services:

Activity	Anticipated Timeline in Calendar Days
Complete onboarding	6-8 weeks
Establish change control procedures	
Deploy all required tools and appliances	10-15 days
Train staff in use of all services	No formal training provided
Integrate with and ingest content from existing tools	10-15 days
Required project meetings	Monthly meetings with the Hospital's Cybersecurity Advisor

Activity	Anticipated Timeline
Define success criteria for solution and deployment	Within three Days of Signing Agreement
Build your tailored installation and deployment plan	First week of Service
Install sensor	Partners schedule
Import Nodes or IPs	Five days after install
Performance baselining	Within the first four to six weeks of Service
SOCVue Walkthrough (Review Incidents, Scan Results, Patches and Reporting)	Within the first month of Service
Alert and report customization	Within the second month of Service
Monthly meeting and review with Dedicated Cybersecurity Advisor	Every month of service

The Cygilant onboarding process is described in more detail below and will be performed in three stages:

### 5. Service Orientation Call

Your Cygilant Account Executive Cooper Mooney will contact you to schedule a Service Orientation Call with your Cygilant Cybersecurity Advisor. The goals of the call will be:

- Introduce the Hospital to the SOCVue Security Monitoring service People, Processes, and Technology
- Identify points of contact



- Define requirements for toolset deployment
- Identify devices on which to monitor
- Provide connectivity requirements for toolset communication

## 6. Installation Call

After your Service Orientation Call has been performed, you will be contacted to schedule the installation of security monitoring solution. The goals of the installation call will be:

- Install the AlienVault USM Anywhere SIEM solution and SentinelOne tool
- Test and validate toolset connectivity
- Integrate nodes to be monitored
- Transition to service deployment

## 7. Service Deployment and Security Monitoring

Further deployment actions will be performed by your Cybersecurity Advisor and the Cygilant Security Operations Center. The subsequent steps will include:

- Review the status of the onboarding project plan
- Validate contacts to receive notifications
- Set up access to the SOCVue platform
- Discuss reporting needs
- Conduct internal operation readiness review
- Commence with security monitoring deliverables as outlined in Section 4: Service Features

During the on-boarding process, Cygilant will work with the Mayer Memorial Hospital IT team to customize the alerts to meet the Hospital needs. Cygilant will work to define what the Hospital considers an Urgent, High, Medium, and Low alert. Each company defines “alerts” differently, so during the onboarding process your dedicated Cybersecurity Advisor will document how you define each severity of alerts. This documentation will act as knowledge base (KB) articles for the account – allowing your dedicated Cybersecurity Advisor and SOC to cross reference and use a baseline. This allows Cygilant to provide the Hospital their desired level of service. This personalization to the alerts and account are included in our services and the Hospital will not be charged extra for this customization.

After the on-boarding process, the Hospital will work directly with both the Cybersecurity Advisor and the SOC to continuously finetune and configure alert rulesets, their playbook, the AlienVault USM Anywhere SIEM technology, etc. – as mentioned above. During these normal operations, if SOC analysis of alerts determines a need for tuning is present or suspected, a ticket will be created to modify customer security content. This is a process of continual improvement in line with the lifecycle of security content management. This continual finetuning allows Cygilant to provide the Hospital District their desired level of service for the entirety of the partnership.

- 22. Describe the overall level of effort and engagement of our internal team to assist in the POC and implementation of your MDR Services. Please include descriptions of all software and hardware installations as well as configuration that the MMHD team will need to assist with.**

Cygilant and the Hospital will maintain a constant ongoing relationship throughout the entire duration of the service agreement, whether through the SOC, Cybersecurity Advisor, Account Manager, or Executive Sponsor. Implementation is handled directly by the SOC and your Cybersecurity Advisor, which is included as part of the service cost. During implementation, the Hospital will join scheduled calls and answer outreach (via phone/email) from the Cybersecurity Advisor or SOC to assist with questions/troubleshooting needed to complete the implementation for the Hospital (i.e. credentials, access to servers for installation, etc.).

With the help of both Cygilant and AlienVault USM Anywhere, the Hospital will configure and set up a server via VMWare for the AlienVault installation. The server requirements for configuring the VMware server are provided by Cygilant prior to our installation call. The requirements provide a step-by-step process including network bandwidth, necessary open ports (only for installation), etc. (<https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/aws/about-usm-aws-sensor-deployment.htm>) See link for server requirements. Once that server is configured, the rest of the implementation is done by Cygilant. After implementation, the responsibilities/resources for both Cygilant and the Hospital can be found below.

#### The Hospital's Responsibilities Include:

- Customer shall cooperate with and assist the SOCVue Services Team in the performance of the services, and will provide the following resources necessary for the SOCVue Services Team's performance hereunder as specified.
- Customer is responsible for maintaining port/protocols required for communication between managed nodes and the security monitoring components (on-premises or cloud-based).
- If remote VPN access is required, Customer shall grant and provide the SOCVue Services Team with secure remote VPN access to the system running the security monitoring platform at all times during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer shall appoint a contact designated to work with the SOCVue Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.
- Customer will promptly communicate to the SOCVue Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any incidents about which they are notified.
- Customer will be responsible for providing the SOCVue Services Team with a complete listing of devices, servers, and applications to be monitored.
- Customer is responsible for procuring the necessary data quota to cover the monthly event volumes transmitted to AlienVault USM. In the event of an overage, Customer is responsible for taking action to reduce data volume or procure additional data in a timely manner.
- Customer is responsible for the cost of storing data beyond the standard 12-month retention period that comes with the purchased subscription level.
- Customer will be responsible for configuring the devices, servers and applications that will be monitored per the SOCVue Services Team instructions.

- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating any security monitoring components installed in the customer's environment.
- Customer must provide the appropriate prerequisite hardware and software necessary for the security monitoring components to be installed and operate properly.
- For on-premises components, Customer is responsible for backups and restore of the solution and all data needed.

Cygilant Responsibilities Include:

- Cygilant will ensure that Cygilant analysts and engineers assigned to the service are knowledgeable about the Cygilant and AlienVault toolsets.
- Cygilant will deliver the service as detailed in Section 4: Service Features.
- Cygilant analysts are responsible for meeting the SLAs in Section 7: Target Service Levels
- Cygilant is responsible for notifying Customer about data overages in a timely manner and giving Customer the option to purchase additional data.
- Cygilant shall retain the collected event log data for 12 months. (Additional storage is available for a fee.)
- Upon termination of cloud-based deployments, Cygilant will retain customer event log data in cold storage for up to 30 days. (Data storage charges apply.)
- Cygilant shall transfer data from cloud storage to the customer upon written request. (Data transfer charges apply.)

**23. What points of ongoing technical integration do you expect we will need to perform?**

To ensure ongoing technical integration, the Hospital will simply need to enable each device (i.e. firewall, domain controller, server, cloud infrastructure, etc.) for monitoring. The AlienVault USM Anywhere SIEM can interface with most existing IT/security products through log delivery and are collected through various mechanisms. Collection mechanisms are primarily syslog and NxLog. If logs can be delivered (usually through syslog) into the SIEM, the expectation is that they will be available to be analyzed for potential security threats. Where the SIEM identifies a potentially security incident based on these logs, they will be presented to the Cygilant SOC within the SOCVue platform. Here is the most updated list of supported sources (AlienApps):

<https://cybersecurity.att.com/documentation/resources/pdf/usm-anywhere-alienapps-list.pdf>

Some examples of logs include: Windows, Linux, Azure, Cisco Meraki, VMWare, PaloAlto, Semantic, BitDefender, etc.

If there is a commissioned device that is not listed on the supported devices list or there is not an active collection mechanism built into the SIEM for that supported technology, Cygilant and the Hospital's Cybersecurity Advisor will open a support ticket with AlienVault USM Anywhere support on behalf of the Hospital's team. AlienVault USM Anywhere will then custom-build a collection mechanism for that unsupported device, to ensure we can parse the log data and allow our SOC team to ingest and monitor that device for alerting purposes.

Any devices can be added or removed by the Cygilant SOC Team and/or the Hospital's Cybersecurity Advisor. All that is required is that their logs are sent to the SIEM, which can be done without any specific input from Cygilant. However, Cygilant asks that the Hospital inform Cygilant as a courtesy if they intend on adding or removing large volumes or noisy devices to ensure the Hospital receives the expected outcomes. The Hospital can inform Cygilant through phone, email, or SOCVue ticket. Subsequently, as long as logs continue to be delivered into the SIEM, service will be maintained.

For the ongoing integration between the Hospital' network and the SIEM technology, Cygilant will perform ongoing patches and updates. Cygilant can coordinate with the Hospital on times for this to occur. As with any system that must get patched, log collection will temporarily halt while the system is being updated or services are restarting.

**24. Does your solution expect/require tools (SIEM, IDS/IPS, AV, EDR, Vulnerability Manager) be in place already?**

No, as part of the service agreement Cygilant will provide access to and install all technologies for SIEM, IDS, AV/EDR and Vulnerability Management. The costs of these technologies are built into Cygilant's overall licensing proposal, attached to this RFP.

**25. What are the total network bandwidth requirements for your solution?**

The AlienVault USM Anywhere SIEM is hosted within AWS, by Cygilant. In order to collect data from the Hospital District – the District will need to download and install a very lightweight data sensor on one of their VMWare servers. The data sensor requires very little bandwidth requirements for the install and ongoing production.

**26. What type of access/permissions will you need to our network?**

Cygilant will need an outbound connection, through one of the District's external firewalls, to establish a connection to the sensor being hosted in the AWS cloud. Once that connection is established, we can start to send logs directly from network devices, cloud infrastructure, etc. to the AlienVault USM Anywhere SIEM.

**27. What redundancies are in place to ensure constant operation of your solution?**

Cygilant Responsibilities Include:

- Cygilant will ensure that Cygilant analysts and engineers assigned to the service are knowledgeable about the Cygilant and AlienVault toolsets.
- Cygilant will deliver the service as detailed in Section 4: Service Features.
- Cygilant analysts are responsible for meeting the SLAs in Section 7: Target Service Levels
- Cygilant is responsible for notifying Customer about data overages in a timely manner and giving Customer the option to purchase additional data.
- Cygilant shall retain the collected event log data for 12 months. (Additional storage is available for a fee.)
- Upon termination of cloud-based deployments, Cygilant will retain customer event log data in cold storage for up to 30 days. (Data storage charges apply.)
- Cygilant shall transfer data from cloud storage to the customer upon written request. (Data transfer charges apply.)

## **28. What redundancies do you expect us to have in place to accommodate constant operation?**

The Hospital's Security Monitoring (AlienVault) Responsibilities Include:

- Customer shall cooperate with and assist the SOCVue Services Team in the performance of the services, and will provide the following resources necessary for the SOCVue Services Team's performance hereunder as specified.
- Customer is responsible for maintaining port/protocols required for communication between managed nodes and the security monitoring components (on-premises or cloud-based).
- If remote VPN access is required, Customer shall grant and provide the SOCVue Services Team with secure remote VPN access to the system running the security monitoring platform at all times during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer shall appoint a contact designated to work with the SOCVue Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.
- Customer will promptly communicate to the SOCVue Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any incidents about which they are notified.
- Customer will be responsible for providing the SOCVue Services Team with a complete listing of devices, servers, and applications to be monitored.
- Customer is responsible for procuring the necessary data quota to cover the monthly event volumes transmitted to AlienVault USM. In the event of an overage, Customer is responsible for taking action to reduce data volume or procure additional data in a timely manner.
- Customer is responsible for the cost of storing data beyond the standard 12-month retention period that comes with the purchased subscription level.
- Customer will be responsible for configuring the devices, servers and applications that will be monitored per the SOCVue Services Team instructions.
- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating any security monitoring components installed in the customer's environment.
- Customer must provide the appropriate prerequisite hardware and software necessary for the security monitoring components to be installed and operate properly.
- For on-premises components, Customer is responsible for backups and restore of the solution and all data needed.

The Hospital's Managed Endpoint (SentinelOne) Responsibilities Include:

- Customer shall cooperate with and assist the Cygilant Services Team in the performance of the services and will provide the following resources necessary for the Cygilant Services Team's performance hereunder as specified.
- Customer shall appoint a contact designated to work with the Cygilant Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.

- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer will notify Cygilant of a change to contact details and provide alternative contacts in times of short-term unavailability.
- Customer will promptly communicate to the Cygilant Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for maintaining port/protocols required for communication between endpoint agents and SentinelOne cloud components.
- Customer will be responsible for providing the Cygilant Services Team with a complete listing of endpoints to be licensed and protected by SentinelOne.
- Customer is responsible for verifying remediation of any incidents detected by the SentinelOne solution.

The Hospital's Vulnerability Management (Qualys) Responsibilities Include:

- Customer shall cooperate with and assist Cygilant in the performance of the services, and will provide the following resources necessary for Cygilant's performance hereunder as specified.
- Customer shall grant and provide Cygilant secure access to the system running the vulnerability scanner during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall ensure connectivity from vulnerability scanning tool and target systems.
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.).
- Customer shall appoint a contact designated to work with Cygilant for all aspects, including escalations, related to the services that will have authority to act on behalf of customer.
- Customer will promptly communicate to Cygilant any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any vulnerability of which they are notified.
- Customer will be responsible for providing Cygilant with a complete listing of nodes to be managed and licensed, along with system credentials if required for a credentialed scan.
- Customer is responsible for procuring necessary node licenses for the vulnerability scanning.
- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating the vulnerability scanner.
- Customer must provide the appropriate prerequisite hardware and software necessary for the vulnerability scanners to be installed and operate properly.
- Customer is responsible for backing up and restoring the solution and all data needed.
- Customer is responsible for maintaining the confidentiality of SOCVue account credentials and is not to share credentials with other users. Cygilant retains the right to terminate access for violations.

**29. Please provide Software and Vendor names for your AV/EDR, IDS/IPS, SIEM, Vulnerability Management Systems, and any other services offered. If you are only offering management of existing services, please list compatible AV/EDR, IDS/IPS, Vulnerability Managers, and SIEM that you are able to manage for us.**

## **SIEM – AlienVault USM Anywhere**

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on premises, and in remote locations, helping you to detect threats virtually anywhere. USM Anywhere automatically collects and analyzes data across your attack surface, helping you to quickly gain centralized security visibility without the complexity of multiple disparate security technologies. With threat intelligence provided by AT&T Alien Labs, USM Anywhere is updated automatically to stay on top of evolving and emerging threats, so your team can focus on responding to alerts. USM Anywhere supports a growing ecosystem of AlienApps, enabling you to orchestrate and automate actions towards other security technologies so you can respond to incidents quickly and easily. It additionally provides main functionalities below:

### Discover

- Network asset discovery
- Software & services discovery
- AWS asset discovery
- Azure asset discovery
- Google Cloud Platform asset discovery

### Analyze

- SIEM event correlation, auto-prioritized alarms
- User activity monitoring
- Up to 90-days of online, searchable events

### Detect

- Cloud intrusion detection (AWS, Azure, GCP)
- Network intrusion detection (NIDS)
- Host intrusion detection (HIDS)
- Endpoint Detection and Response (EDR)

### Respond

- Forensics querying
- Automate & orchestrate response
- Notifications and ticketing

### Assess

- Vulnerability scanning
- Cloud infrastructure assessment
- User & asset configuration
- Dark web monitoring

### Report

- Pre-built compliance reporting templates
- Pre-built event reporting templates
- Customizable views and dashboards
- Log storage

Refer to AT&T website for information: (<https://cybersecurity.att.com/products/usm-anywhere>)

### ***IDS – AlienVault USM Anywhere***

AlienVault NIDS plays an important role in the USM Anywhere SIEM technology and provides contextualized alerting directly to our SOC through its built-in function. By detecting malicious network events, it provides vital information for correlation directives and cross-correlation rules. Combining this information with the events collected from other devices, USM Anywhere presents a complete picture of the malicious activity.

The AlienVault NIDS functionality, including monitoring network traffic and detecting malicious events, takes place on the USM Sensor. The USM Server consumes the NIDS signatures through plugins, which generates the AlienVault NIDS events. The correlation engine processes and correlates the normalized events, then stores them in the SIEM database.

Refer to AT&T website for information: (<https://cybersecurity.att.com/documentation/usm-appliance/ids-configuration/about-alienvault-nids.htm>)

### ***AV/EDR – SentinelOne***

The SentinelOne EDR platform unified prevention, detection and response in a single purpose-built agent powered by machine learning and automation. It provides and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into endpoint environment with full context, real-time forensics. This protects Windows, Mac and Linux.

SentinelOne Complete features include:

- Endpoint Prevention (EPP) to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start.
- ActiveEDR Basic for Detection & Response (EDR) works in real time with or without cloud connectivity. ActiveEDR detects highly sophisticated malware, memory exploits, script misuse and other fileless attacks as they attempt to do damage. ActiveEDR responds at machine speed to autonomously contain damage
- ActiveEDR recovery gets users up and running in minutes and includes 100% remediation as well as rollback for Microsoft Windows
- Device Control for policy-based control of all USB device peripherals
- Firewall Control for policy-based control of network connectivity to and from assets, including location awareness
- Full Remote Shell capability for direct endpoint access by incident responders and forensics personnel

Refer to SentinelOne website for information: (<https://www.sentinelone.com/platform/singularity-control/>)

### ***Vulnerability Management – Qualys***

#### **30. Do you threat hunt 24x7x365?**



Cygilant has developed a 24x7x365 Security Monitoring service that addresses the significant challenges of security monitoring products:

- Managing the complexity of SIEM and Log Management products
- Lack of trained personnel to manage SIEM and Log Management products
- Difficulty of gaining useful or meaningful information from SIEM and Log Management products

SOCVue® Security Monitoring is a subscription-based service that delivers the proper people, process, and technology for an effective security program. Cygilant Cybersecurity Advisors (CA) will install and manage the AlienVault USM solution, and the Cygilant Security Operations Center (SOC) will continuously monitor and make customers aware of potential security incidents.

The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6).

The key benefits that SOCVue Security Monitoring delivers to customers are:

- 24x7x365 Continuous monitoring of log and event data to detect potential security incidents
- Integrated network intrusion detection (IDS), file integrity monitoring (FIM), and threat intelligence feeds
- Timely investigation and notification about incidents that need attention
- Reporting on security events and alerts
- Assistance with compliance needs regarding FFIEC, PCI DSS, HIPAA, and other regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with your Cygilant CA covering the customer's overall security posture and overall system health

**31. During off hours is it an on call staffing or are there live analysts in SOC 24/7?**

During off hours, Cygilant has 24x7 live SOC analysts staffed to support the needs and concerns of the Hospital District. They can be reached via direct phone or via email ([soc@cygilant.com](mailto:soc@cygilant.com)).

**32. Are there times you do not provide monitoring services?**

No, Cygilant will monitor Mayer Memorial Hospital District 24x7x365.

**33. How many technical staff members do you have in total between all SOCs?**

Cygilant has 35 security professionals globally.

**34. Are analysts and engineers allocated evenly over shifts?**

No, Cygilant SOC members, both analysts and engineers, are assigned in alignment to a few different factors:

- Busy and quiet periods of alert generation
- Customer hours of business
- Backlog of security engineering work
- Response to customer escalations
- Response to threat intelligence and significant immediate threats

**35. What Information Technology and Information Security certifications are held by your staff? Please list how many of each certification.**

Our staff have a range of industry standard certifications including from CompTIA, Microsoft, and courses in cyber security from accredited universities.

**36. How do you keep your staff current with technology?**

Cygilant SOC Analysts are trained in our internal and 3rd party partner tools as standard. Additional technology added to our service delivery is supported by appropriate training

**37. Do you allocate time for your staff to attend training and/or obtain additional certifications?**

Cygilant trains security analysts internally by using a combination of on-the-job shadowing and internal training resources to ensure analysts are fully equipped to analyse incidents and follow Cygilant’s internal processes and systems. Training is provided for staff on a regular basis to support continual improvement, and certifications are supported when needed to formalize ongoing development.

**38. What’s your average response time?**

Severity	Action	Service Desk Request Targets	Security Monitoring Targets
P1 - Critical	Acknowledgment*	Within 15 minutes	Within 15 minutes
	Response Time**	Within 30 minutes	Within 15 minutes
	Escalation to Manager	Within 2 hours	Within 2 hours
P2 - High	Acknowledgment	Within 30 minutes	Within 30 minutes
	Response Time	Within 1 hour	Within 30 minutes
	Escalation to Manager	Within 4 hours	Within 4 hours
P3 - Medium	Acknowledgment	Within 3 hours	Within 1 hour
	Response Time	Within 6 hours	Within 2 hours
	Escalation to Manager	Within 24 hours	Within 24 hours
P4 - Low	Acknowledgment	Within 8 hours	Within 2 hours
	Response Time	Within 24 hours	Within 4 hours
	Escalation to Manager	As Required	As Required

\*Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation.

\*\*Response time is the elapsed time from Acknowledgement to confirmation that a SOC Analyst is investigating the issue

**39. What’s your average time to resolution?**

Please refer to above answer to question no. 38.

**40. Can I call into the SOC? Will I speak to an automated phone tree/scheduler?**

For urgent issues, the Hospital will be given a direct phone line and email ([soc@cygilant.com](mailto:soc@cygilant.com)) to the SOC for any outstanding issues/concerns – and have access to this phone line/email on a 24x7 basis. The 24x7 SOC and an analyst will address those issues in real-time within our outlined SLAs. Therefore, the Hospital can reach out to and work directly with a SOC team member avoiding an automated phone tree/scheduler, as described above.

During normal business hours, the Hospital can raise any questions and concerns by 1) reaching out to their dedicated Cybersecurity Advisor via phone and email to ask for assistance on

ongoing issues. If the Cybersecurity Advisor decides your issue needs to be escalated to the SOC, he/she will do so on your behalf and work with you until your issues are entirely resolved. 2) open a ticket in our SOCVue platform. The SOCVue platform will allow you to:

- View and manage alerts and incidents
- Initiate and manage tickets
- Track remediation outcomes
- Access security and compliance reporting

**41. Do you perform background checks on your employees with access to customer information?**

All Cygilant employees undergo full, enhanced background checks.

**42. Will anyone ever access my data or perform investigations outside a secure environment (i.e. Home office, etc)**

Your Cybersecurity Advisor will have access to both your SOCVue platform instance and your SIEM technology. However, there are security processes in place to ensure the security of the Hospital's data. Logs are encrypted in transit from the LogPoint collector to the LogPoint backend using Transport Layer Security (TLS) encryption. Alert data is encrypted in transit from the LogPoint backend to Cygilant using TLS. Log data stored in the Cygilant cloud is encrypted at rest using 256-bit Advanced Encryption Standard (AES).

**43. Please describe your process for providing security for systems that cannot be secured to best practices, such as legacy systems that have not been replaced yet.**

Best practice is always contextual, and Cyber Security is an exercise in Elastic Defense (Castle Defense / Defense in Depth) - Layers of security, not just a single line. The essence of this starts with doing the basics well. i.e., Regular Scans for Vulnerabilities, Manage Patching, Protect Endpoints, Monitor Systems, Continual Review & Improvement, Plan Actions for Response, etc.

Our security services are designed to cover these basics, to give an in depth defense against compromise, which works in partnership with your security program - Especially when some measures can't be taken (E.g. Awareness of XP vulnerabilities on POS devices via Qualys → CSA Team Advise upgrade path → Can't because of system driver support → CSA advises strategy to protect in multiple layers → Firewall / UAC / System Hardening / Best Practice Checks → Deploy Sentinel One Legacy Client for windows XP → Configure log monitoring → Regularly review status of high value / risk targets → Advise on future upgrade path.

**44. Is security event data shared across your customer base? How is this handled to ensure confidentiality and HIPAA compliance?**

Cygilant's SOCVue logically separates user data throughout its life cycle by marking/associating it with a code that is uniquely assigned to each customer. This code is used to logically differentiate, store, and retrieve data during all SOCVue operations. Authorization checks prevent a customer from accessing the data of another customer.

Furthermore, all data collected, processed, and stored by Cygilant is secured using industry best practices including encryption in-transit and at-rest, secure development practices, change control methodologies, and employee screening. Cygilant security controls are audited regularly and

certified for SOC 2 compliance. Any third-party products used by Cygilant to deliver the service are SOC 2 and/or EAL 2+ certified.

**45. How do you intend to help MMHD mitigate the impact of supply chain attacks?**

Cygilant’s services provide defense in depth, with multiple layers of protection and detection at different points in our customer’s environments. This gives us the capability to detect lateral movement / post compromise activities, even against zero-day supply chain attacks. We monitor threat intelligence sources to learn of any new threats on IT supply chain assets and take immediate action to investigate and understand them when they are revealed. Following on from this, we undertake activities to add new detection for indicators of compromise, while working with our customers who may have been exposed to review their systems historically for any signs of exploit. Finally, our CSA team can work with your IT and internal security teams on ways to harden your own deployments, to include suppliers which align to standard such as SOC2, PCI, and ISO27001, all of which decrease your risk.

**46. How do you handle onboarding and visibility of Cloud/SaaS environments such as O365 or cloud based EHRs?**

The Hospital District will work directly with both the SOC team and their Cybersecurity Advisor for the onboarding and visibility of Cloud/SaaS environments such as O365, etc. The Hospital District will notify their CSA of certain cloud environments that they would like to be monitored. As a result, the CSA will start to collect and ingest that data through the AlienVault SIEM and the SOC team will set certain alert rulesets that coincide with the Hospital District’s preferred method of monitoring and other rulebooks already in place with the Cygilant SOC.

**47. How do you monitor endpoints?**

Cygilant will monitor all Mayers Memorial Hospital District’s endpoint through our 24x7 Security Monitoring and Endpoint Management services. Both services are monitored and maintained by Cygilant’s 24x7 global SOC, through the utilization of the AlienVault USM Anywhere SIEM Technology and SentinelOne EDR. We collect log and activity data either directly from the endpoint itself or through SentinelOne’s EDR platform – for further analysis and investigation. All of the District’s servers and workstations are fed through SentinelOne’s EDR product – endpoints other than servers and workstations can be fed through the AlienVault SIEM. Those endpoints being fed through SentinelOne are monitored as followed:

SentinelOne Control is a Next Generation AntiVirus combining Endpoint Protection Platform (EPP) and EDR on a single agent. Static AI replaces traditional signatures and predicts malicious files. Behavioral artificial intelligence (AI) identifies and stops fileless attacks in real time. Autonomous and automatic threat responses trigger protective actions. SentinelOne also includes one-click remediation of unauthorized changes and one-click rollback to restore Windows systems affected by an attack. SentinelOne Control also includes:

- Network Control – policy-based control for inbound and outbound traffic on Windows, Linux, and Mac.
- Device Control – granular control for USB and Bluetooth on Windows and Mac.
- Rogue Device Discovery – uses passive and active sweeps to detect devices that are not

protected by SentinelOne.

The SentinelOne data is then fed through and collected by the AlienVault USM Anywhere SIEM. Depending on the alert rule of SentinelOne and alerts generated by the SIEM, the SOC will monitor these alerts for the Hospital District. Therefore, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. By feeding the SentinelOne EDR produce through the AlienVault SIEM, the SOC team can cross correlate activity across the District's entire environment. Therefore, Cygilant's SOC teams provides better alerting, threat monitoring and will achieve full, 24x7 network visibility.

#### **48. How do you monitor networks?**

Similarly, to how Cygilant monitors the Hospital District's endpoints, we can monitor their networks through our 24x7 Security Monitoring service. Cygilant collects all log and event activity directly from every network device and cloud application/infrastructure on Mayers Memorial Hospital District's network. All the log and event activity are fed through the AlienVault USM Anywhere SIEM technology for security contextualization and analysis. The alerts generated by the SIEM technology are sent directly to Cygilant's SOCVue Platform which platform ingests 5 different Threat Intelligence feeds for further investigation. In real-time and on a 24x7x365 basis, the SOC team will monitor all alerts and activity across the Hospital Districts networks. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

#### **49. What (if any) access to Firewalls are necessary to adequately monitor?**

There will be no access needed from the Hospital District's firewalls for Cygilant's Security Monitoring service and the 24x7 SOC team to adequately monitor them. The Hospital would have to forward the log data – either via syslog or NxLog – to the AlienVault data collector (sensor). This data is then transmitted to AlienVault USM Anywhere for processing/threat intelligence/parsing/etc. Alerts generated by the AlienVault SIEM are collected by the cloud based Cygilant SOCVue platform for review by the SOC.

If the Hospital District has any firewalls owned and maintained by a third-party vendor, Cygilant will need approval and access from that third-party vendor to send log data from those firewalls to the AlienVault sensor.

### **4.d MDR**

#### **50. Do you offer different service level options for security monitoring/alerting?**

No.

**51. If yes, what service level option are you quoting for?**

Please refer to my answer to No. 50.

**52. Does your service include a process for adding new rules/event correlations/sources? If yes, please explain your approach for communicating and gaining approval for these recommendations.**

The District will have ongoing monthly meetings with the assigned Cybersecurity Advisor to review open tickets and incidents, analyze alert rules, discuss event correlations, reporting needs and future deployment plans, and schedule follow-up calls as needed. They will also engage in discussions around current sources being collected and sources to add/remove from the service. These types of changes will frequently be discussed in these meetings. If a change is within the scope of the existing agreement, the Cybersecurity Advisor, with the Districts' permission, will be able to make those changes accordingly. If the change is a new feature and there is a cost involved, the Cybersecurity Advisor, Cygilant Account Manager, and District's team will discuss, agree on, and make changes based on what is in the best interest of the customer.

**53. How often are signatures and threat intel updated?**

Signatures and threat intelligence are updated based on new and evolving threats. Depending on the SIEM or MDR platform, regular updates can range from once a month to several times a week. For significant emerging threats impacting our customer base (E.g. Hafnium, SolarWinds, Kaseya), we seek to deploy security content as soon as it is available, outside of release schedules, E.g. less than 24 hours in some cases.

**54. How do you classify/prioritize security events?**

<b>Severity</b>	<b>Description</b>
P1 – Critical	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be an ACTIVE threat against business impacting customer assets.
P2 - High	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a PROBABLE (current, possible impact) threat against business impacting customer assets.
P3 - Medium	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting customer assets.
P4 - Low	An Incident identified either by automated correlation rules or through SOC analysis that may require further investigation, with no apparent threat against business impacting customer assets.

**55. What is your process for detecting and responding to a threat?**

The SOC team will continuously investigate and triage any alerts or incidents occurring on the Hospital's network to ensure there is no real threat to their security or network. This investigation begins at the SIEM level – configuring and finetuning the technology to trigger alerts for suspicious activity or security violations. These alerts are investigated on a 24x7 basis by Cygilant SOC analysts through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. If an alert generated by the SIEM technology requires further investigation by a SOC analyst, rather than being ruled out as a false positive, white noise, etc. the SOC analyst will create an incident and begin investigating that alert. Through these incident review processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. After an incident has been fully investigated by our SOC and is needed to be escalated to the Hospital District, the SOC team will open a “ticket”.

Dependent on customer handling preferences and the analysis done by the SOC, the SOC will provide actionable remediation guidance to be able to respond to the outstanding threat. If there are steps able to be taken utilizing both the SIEM technology and SentinelOne – depending on customer handling preferences – the SOC can respond in alignment with those processes.

#### **56. How are events sorted between positive and false positive?**

Customer onboarding includes a period of configuration and baselining, which allows us to configure the SIEM alerts to be relevant and vastly reduce false positives. During normal operations, if SOC analysis of alerts determines a false positive is present or suspected, a ticket will be created to modify customer security content to eliminate it. This is a process of continual improvement in line with the lifecycle of security content management. (NB. False Positive is explicitly defined here as being a detection / content issue... I.e. an alert was raised saying “X has been detected” when X was not present - NOT a true positive alert, of low / no security threat or value.)

#### **57. What is the turn-around time from detection to remediation, on average?**

For our MDR service, the average time is almost immediate, because most remediation activities are automated in the platform, before additional analysis or review where needed. This process is tuned during onboarding to avoid operations interruptions on business-critical systems and software.

#### **58. How do you teach your clients to improve their security postures?**

Cygilant teams, both the Cybersecurity Advisor (CSA) and the SOC team, work with our customers on constantly updating our knowledge of their environment and their risk profiles. During these regular reviews, the Cybersecurity Advisor will seek to identify the highest priority security risks through dialog with the customer. Cygilant will also build a knowledgebase about authorized admins and “normal” activity on the network. These regular reviews with your CSA will be conducted monthly meetings with your team. The goal of those meeting is to discuss how you can improve your cybersecurity posture – i.e. reducing incident response time, generating better alerts coinciding with your security objectives, relying on your CSA as an “advisor” to ask question about

improvement, etc. We want to give you access to the security experts (CSA and SOC) so that we can not only meet your security objectives, but also grow and improve them.

**59. How do you improve monitoring capabilities over time based on event history?**

All Cygilant SOC services are based on the principle of continual improvement. Our MDR service is regularly updated with new alert content, based on historical events and the changing threat landscape (new threats). Our analysts continually look for improvement opportunities, from all points of our operations and analysis workflows. In parallel, the MDR service platform and endpoint agents use machine learning techniques to continually monitor for and respond to zero day / unknown threats.

**60. Does your proposal include 24x7 hunting for threats(including zero day threats) within our environment?**

The SOC provides 24x7 threat monitoring of event logs and alerts. Threat intelligence staff at Cygilant will develop new security detection content when new zero-day threats are announced. We often deploy new detection policies even before our security vendor partners are able to release updates to the products. In these situations, the SOC will perform proactive hunts in your environment if there is a possibility that the zero day may have been exploited before being discovered by the industry and disclosed publicly.

**61. How do you perform this hunting?**

Threat hunting is performed using inbuilt tools inside our MDR.

**62. Is there any special software we need to deploy to support this hunting?**

Yes, the Sentinel One agent must be deployed on all monitored endpoints, alongside log collectors on servers. This software is included in the cost proposal attached to the RFP above.

**63. What part do humans play in the threat hunting lifecycle?**

Humans are a core component of threat hunting, using their knowledge and expertise to identify potentially suspicious activity over and above what pre-determined analytics or machine learning can spot. Our threat hunting is aided by the tools available, but is very much built around human processes and insight

**64. Describe your methodology for remediation on our behalf and how notification of these actions will be handled.**

Our MDR platform implements proactive blocking and quarantine of malicious threats. It also supports detection of threats which are deemed suspicious, which are available for an analyst to choose to kill or quarantine from the console. In both cases customers are notified about all actions taken. Depending on customer preference we can put in place escalation requirements before analysts actively kill / quarantine or can edit the detection logic to whitelist activity.

## **4.e Incident Analysis and Response**



**65. Do you perform real-time inspection of every packet utilizing full packet capture? If you do full packet capture please explain how long you do it for, when it starts, and how long you retain it for?**

Cygilant cannot perform this type of activity, but we can leverage our Cygilant partners on a separate retainer that can accommodate these requests. Retainers for our partners can be discussed as an add-on to Cygilant's services. Our partners' retainers are not included in the cost proposal of this RFP.

**66. Does your solution detect unknown threats and attacks leveraging patterns and behavioral analytics?**

Our MDR service contains both signature and machine learning / AI backed detection which is able to identify anomalous and suspicious behavior without advanced signature knowledge of the malicious activity.

**67. Does your solution detect based on signatures and IOC's?**

Yes, our SIEM and MDR have the ability to detect or block activity based on emerging IoCs, signatures and correlation rules defined by the vendor or by Cygilant.

**68. Do you do full forensic analysis to confirm threats and eliminate false positives?**

Cygilant analyzes the information available inside the systems based on the data being passed to us from the customer network. This data is inspected to confirm the existence of a threat over and above whatever information is available in an alarm directly. It is also used to support recommendations for whitelisting / suppression of benign activity inside the customer environment. We do not have access directly to hosts for the purposes of investigation and require partnership with the customer where additional information must be gathered.

**69. Are you able to do near real-time communication disruption and isolation of threats on client's behalf?**

Our MDR service has the ability to isolate a potentially infected host from the network entirely while retaining MDR access or to enact firewall rules to block network communication with destinations based on the threat.

**70. If so, are these placed autonomously or by human decision? If both please specify when and how the decision is derived.**

It is possible to configure the MDR to automatically enact these reactions to malicious threats. Generally, this not how our MDR customers have the system configured and it is left to analyst discretion on a case-by-case basis. Given that the MDR kills and quarantine a threat, then it is unusual for us to suspect additional activity on the host such that isolation or firewall blocking is immediately required outside of the customer directing us to enact that. Therefore, those actions are taken after customer engagement if the customer requests it for additional mitigation. This arrangement is open to change based on customer preferences.

**71. Please describe the level of support provided until incident is remediated and threat actor is eliminated.**

The SOC is available to provide insight and analysis of data which is present in the SIEM. We will liaise with any external forensics team or internal remediation team for the customer as needed. The SOC will be on hand to analyze the data at the Hospital Districts disposal until the issue is resolved.

**72. Do you charge retainers or extra fees on top of your base costs for this incident response capability? If so, please elaborate on what this entails and how you charge for these services**

We do not support services for forensics / incident response directly. Should this service be needed we have a partnership with Incident Response companies who can be engaged for additional fees. We will then work directly with that IR organization and yourselves regarding incident response based on the information we have available inside our systems.

**73. What would constitute a variable bill?**

Cygilant does not charge via variable bill, these costs are built into our annual cost of our services. If we need to engage in a retainer with an Incident Response partner, those costs will depend on that partner.

**74. At what point do you engage MMHD's Information Security Staff to assist?**

Should activity be blocked by our MDR then the District would be notified after the fact that it has occurred and may be asked to carry out further investigation to conclude that no additional threat persists. Should activity be detected by the SIEM and an analyst has evaluated it as a valid threat requiring further remediation then this will be raised to the Hospital District for further assistance.

**75. What does your normal escalation and notification process look like?**

The SOC team will continuously investigate and triage any alerts or incidents occurring on the Hospital's network to ensure there is no real threat to their security or network. This investigation begins at the SIEM level – configuring and finetuning the technology to trigger alerts for suspicious activity or security violations. These alerts are investigated on a 24x7 basis by Cygilant SOC analysts through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. If an alert generated by the SIEM technology requires further investigation by a SOC analyst, rather than being ruled out as a false positive, white noise, etc. the SOC analyst will create an incident and begin investigating that alert. Through these incident review processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. After an incident has been fully investigated by our SOC and is needed to be escalated to the Hospital District, the SOC team will open a "ticket".

"Tickets" are actionable security related incidents or custom alerts that the SOC team has escalated directly to the Hospital District for action needed to be taken to remediate or needed interaction between the Hospital and the SOC. The severity of these tickets can range from "Critical to Low" dependent on the severity of the event determined by the SOC and customer handling preferences. The Hospital will decide with their Cybersecurity Advisor and the SOC team

during onboarding to determine how they prefer to be notified, either via phone call or email. The Hospital District can also determine a chain of command within their IT team as part of the ticketing process to ensure that the SOC will reach an IT team member at the Hospital District and notify them of the security incident.

Every “open ticket” (i.e. tickets that are unresolved between the SOC and the Hospital District) are integrated with our SOCVue platform to be worked-on and viewed by the Hospital District. The SOCVue platform is a multi-tenant interactive platform created and developed by Cygilant. The purpose of SOCVue is to provide the Hospital District a single pane of glass to simplify and consolidate multiple streams of security data to help detect and respond to threats faster. It will allow the Hospital District to view and manage alerts and incidents, initiate, and manage tickets, track remediation outcomes, and access security and compliance reporting. The SOC team works in the same SOCVue platform as the Hospital District to provide direct, customizable alerts. Therefore, the Districts are alerted on both critical security-related incidents and any customizable alerts desired. Also, by working in the same platform, the Hospital District can see Cygilant’s SOC threat hunting and monitoring processes in real-time.

At a high level, SOCVue provides an overarching view of the Districts’ entire environment for complete network visibility, portrayed through dashboards. The dashboards provide meaningful information about network activity without having to dive deeper into alerts or incidents. Examples of these dashboards include: Nodes being collected from, Assets at Risk, Top Source and Destination IPs, Alerts by Severity, and Average Time to Incident Resolution. However, the SOCVue platform also allows the Hospital District a granular view of their environment all the way down to the raw log if needed.

In the SOCVue dashboard, there will be an “open tickets” drilldown. This drilldown will provide all of the open tickets that are either security-related incidents or custom alerts that have been escalated by the SOC team to the Hospital District. By simply responding to these tickets, the Districts and the SOC will resolve and close out that security related incident or custom alert. However, the Districts can further drilldown into that ticket to both the incident and the alert level. In the incident drilldown, the SOC will provide information on the time of the alert, affected system, probable cause, impact, best practices and suggested remedy. This shows the forensic analysis done by the SOC to ultimately escalate this incident to an alert. Furthermore, in the incident drilldown, the Hospital District will be able to dive deeper all the way down to the Alert Drilldown. In the alert drilldown, the Hospital District will be able to get information about the alert that triggered the incident, down to the raw log itself.

Please see attached photos of our SOCVue platform:

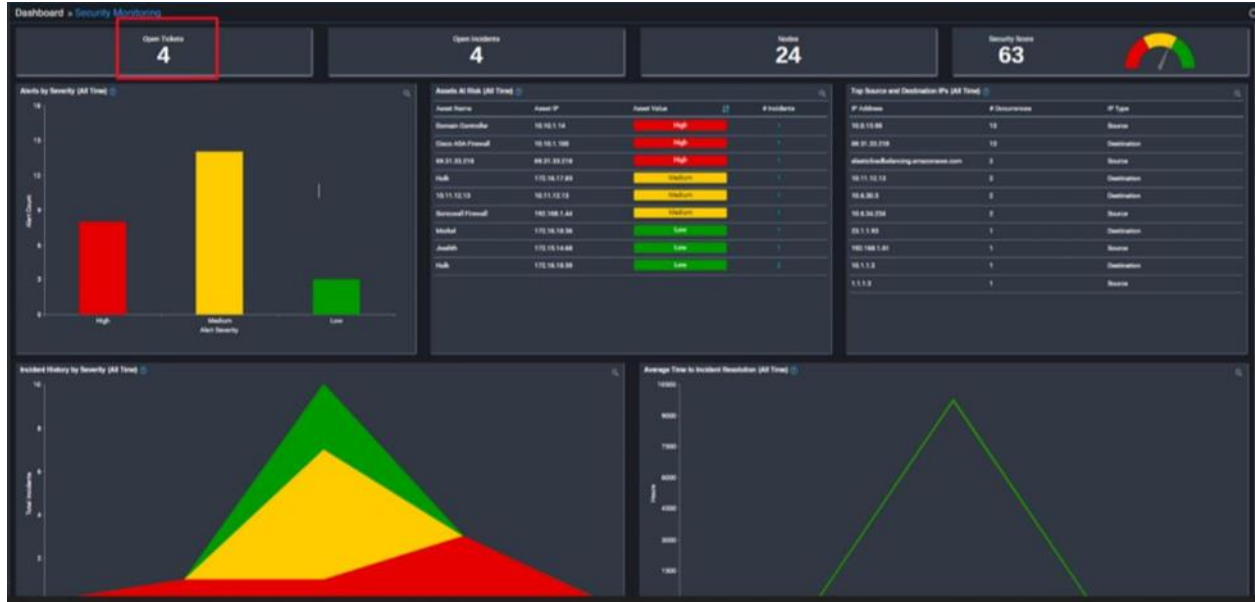


Figure 1: SOCVue Dashboard View

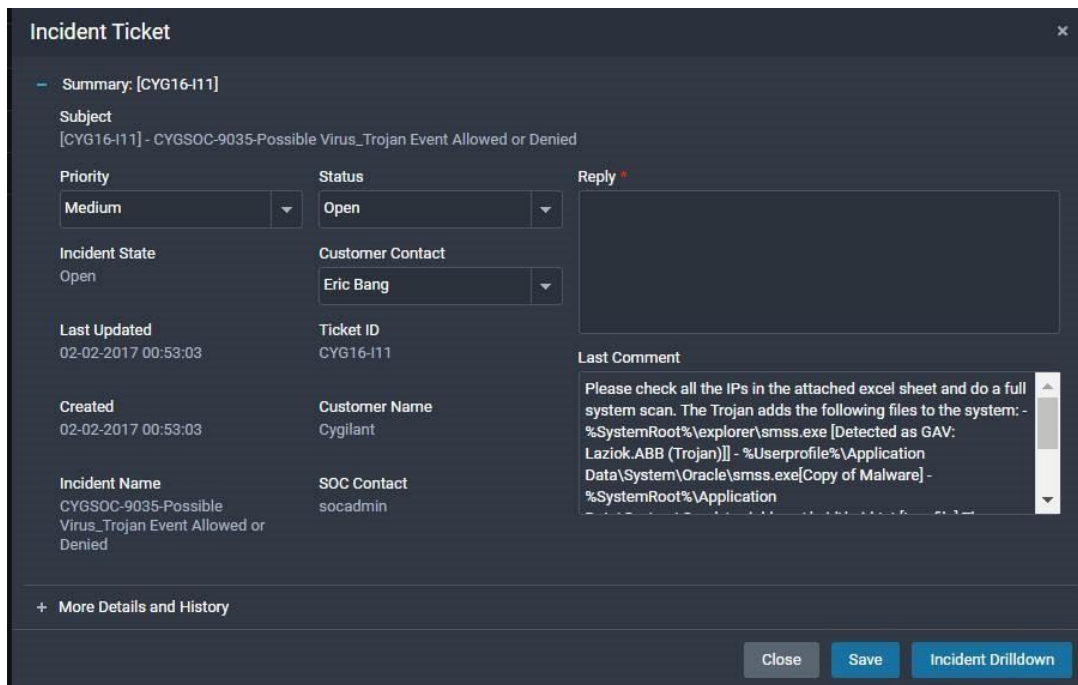


Figure 2: Incident Ticket

### Incident Details

<b>Id</b> CYG16-111	<b>Type</b> Incident	<b>Severity</b> High	<b>First Occurrence Time</b> 10-09-2018 20:00:00
<b>Name</b> CYGSOC-9035-Possible Virus_Trojan Event Allowed or Denied	<b>State</b> Open	<b>Alert Code</b> 9035	<b>Last Occurrence Time</b> 10-09-2018 20:00:00
<b>Code</b> CYG16_111	<b>Reported At</b> 10-09-2018 20:00:00	<b>Alert(s) Triggered Count</b> 1	<b>Repeated Count</b> 0
<b>SOC Contact</b> Cygilant SOCAAdmin	<b>Time Zone</b> (GMT-05:00) Eastern Time(US & Canada)		

**Affected System(s)**

IP	System Name	Type	Asset Value
192.168.1.44	Sonicwall Firewall	Sonicwall	Medium

**Probable Cause**

We have seen multiple internal IP addresses triggering a SonicWall IPS alert about a malware signature \*\*GAV: Laziok.ABB\*\*

**Impact**

Risk of data exfiltration. The volume is huge and it will also impact the IPS performance.

**Best Practice**

Run regular A/V scans.


**Suggested Remedy**

Please check all the IP's in the attached excel sheet and do a full system scan.

The Trojan adds the following files to the system:

Close Alert Drilldown Ticket Drilldown

Figure 3: Incident Ticket Details



Cygilant | cmooney@cygilant.com

Security Monitoring » Incidents

Incidents Alerts Grouped Alerts

0  
Open Incidents

3  
In Progress

1  
Pending Customer

1  
Pending SOC

0  
Monitoring

+ New Edit Advanced Filter All Time Group Action All Time

Customer Name	Incident ID	Name	Severity	Threat Indicator	Alert(s) Trigger...	Repeated Count	Reported At	Last Occurrence	Ticket	SOC Contact	Incident State	Action
Cygilant	CYG20-H2	Windows Elevated Privileg...	Medium		0	0	12-01-20 13:38	12-01-20 00:00		Kevin Landt	Open	
Cygilant	CYG19-H2	CYG-110118-AWS Configu...	High		1	0	01-02-19 14:23	01-02-19 14:23		Andy Igel	In Progress	
Cygilant	CYG19-H1	CYGSOC-9035-Possible Vi...	High		1	0	01-01-19 05:00	01-01-19 05:00		Andy Igel	In Progress	
Cygilant	CYG16-111	CYGSOC-9035-Possible Vi...	High		1	0	10-09-18 20:00	10-09-18 20:00		Andy Igel	Open	
Cygilant	CYG16-112	CYGSOC-15009-TCP DoS ...	Medium		1	0	10-09-18 20:00	10-09-18 20:00		socadmin	In Progress	
Cygilant	CYG16-113	CYGSOC-1018-Member w...	Low		1	0	10-09-18 20:00	10-09-18 20:00		aigel	Pending Cust...	
Cygilant	CYG18-H2630	CYGAVT-50004-Configurat...	Medium		1	0	10-03-18 06:47	10-03-18 06:47		Andy Igel	Open	
Cygilant	CYG18-H2629	CYGAVT-50004-Configurat...	Medium		1	0	10-03-18 05:00	10-03-18 05:00		Andy Igel	Open	
Cygilant	CYG18-H2623	CYGAVT-50004-Backdoor...	Low		1	0	09-27-18 05:12	09-27-18 05:12		Twinkle Cha...	Pending SOC	

Go to page: 1 Show rows: 10 1-10 of 10

Figure 4: SOCVue Incidents List

## 76. Does your service provide full response reports on investigations?

CYGILANT, INC

33

Should a customer require a formal report about activity from an investigation of a potential breach then that can be provided after the investigation concludes and any remediation activity has been carried out.

**77. How quickly can a full breach report be developed so we can notify affected individuals?**

This would be dependent on the complexity of the investigation and what activity needs to be performed by an Incident Response partner of Cygilant's. We are happy to engage with supplying information and narratives to the construction with such a report with our Incident Response partners. We have a list of partners we can engage, and the District can choose from.

## **4.f Metrics, Reporting and Dashboards**

**78. Do you provide operational reports to your customers?**

Cygilant creates monthly scorecards as well as executive reports that are generated on a regular cadence and sent directly to the customer. Your Cygilant Cybersecurity Advisor will review the options with the Hospital during onboarding. Some examples include monthly executive summary, compliance reports (HIPAA, NIST, etc.) for auditing, and monthly scorecards.

We have standard reports as well as we can create ad-hoc/custom reports based on the requirements needed to your liking. These reports can be adjusted to daily/weekly/monthly as an example.

AlienVault USM Anywhere generates these reports:

- **My Reports** - These reports are generated from your report creation feature and are selectable by categories, which are assets, asset groups, alarms, events, vulnerabilities, and configuration issues. You can also choose the format of the report (HTML and CSV).
- **Compliance Templates** - These are compliance templates based on alarms, vulnerabilities, and events collected in the system. The templates are grouped into PCI, NIST CSF, HIPAA, and ISO 27001. See USM Anywhere Compliance Templates.
- **Event Type Templates** - These are event templates based on event categorization by type of data source and by the most used data sources, see USM Anywhere Event Type Templates.

•

**79. What is the frequency for customer reporting?**

The Hospital can reach out to the Cybersecurity Advisor as many times during the partnership for any type of reports they would want to be generated and can also run their own ad-hoc reports at their own discretion. These unlimited reports are included in the agreed upon service contract. The monthly SOC reports/scorecards are generated on a monthly based and discussed as part of the monthly meetings with your Cybersecurity Advisor. The Hospital can also propose changes to the monthly SOC reports to generate new data

**80. Can you provide sample reports?**

Sample monthly SOC reports are attached on pages 47-53 of this RFP. The report attached is customized to the client's environment, needs and security objectives.

**81. What is your preferred method for delivery of customer reports?**

The preferred method for the delivery of customer reports is our SOCVue platform. The reports the Hospital requests will be imported into the "Reports" tab of our SOCVue portal for historical and logging purposes. The Cybersecurity Advisor will also generate and deliver monthly reports and ad-hoc reports directly to the customer, as requested.

If the customer would like to run their own ad-hoc reports by logging into the back-end SIEM – aforementioned above, they can generate those reports in real-time and download those reports as necessary.

**82. Are real time data and operational reports exportable? If so, what formats are supported?**

The Hospital can export real-time data and operational reports via the back-end AlienVault USM SIEM technology as well as our Cygilant SOCVue portal. All data and reports are exportable via PDF, HTML, CSV, etc.

If the Hospital would prefer the data and reports be exported by their Cybersecurity Advisor, they can reach out to that Advisor and request the data and reports as necessary.

## **4.g Data Management**

**83. Where does my data reside?**

Cygilant maintains strict written information security and confidentiality policies that ensure security controls are in place to protect customer data. These policies and employee training practices are audited by a third party for SOC 2 compliance. These documented policies include, but are not limited to, the following areas, which are reviewed and updated on a regular basis: Physical Security, Access Controls, Software Development Lifecycle, Data Retention, Backup Policy, Configuration Standards, Incident Handling, and Acceptable Use. Cygilant's Security and Compliance Manager works with business groups within the company to ensure implementation and auditing.

Furthermore, Cygilant hosts the AlienVault USM Anywhere instance and customer data in AWS Northeast. Cygilant would house the main SIEM back end in AWS and a smaller lightweight data collector for AlienVault would be set up to facilitate the collection of logs/events to forward to the cloud based SIEM. The installation of the sensor is either on a VMWare or HyperV server – and based on the Hospital's network, the sensor will be installed on VMWare. Furthermore, Cygilant purposefully hosts in AWS – to ensure the safety of customer data.

**84. Data retention: How long will your company store data collected/created?**

The Districts data will be collected and stored in AWS for the entire duration of the contract. Event logs will be available in AlienVault USM for analysis and reporting during the Hot Storage period. The Hot Storage period is 15 Days, 30 Days, or 90 Days depending on your purchase agreement. After the Hot Storage period, logs will be archived and will no longer be available for the Cygilant SOC team to search, report or provide forensics on. However, the logs are still available for

the customer to download and utilize on their own. Logs will be archived for a total of 12 months from the collection time.

To help meet compliance requirements, event log data will be archived in cloud storage beyond the hot storage search and report timeframe. The archived data will not be immediately available for analysis and reporting. Archived data will be provided to the customer in CSV format upon request within 3 business days (Data transfer charges apply). Logs will be retained for a total of 12 months from the collection date. Additional storage beyond 12 months is available for an additional fee.

**85. Data destruction: What is the process for purging or destroying historical data after use?**

Events and log data collected by AlienVault are kept in hot storage for the time period you select (15, 30, or 90 days) and then purged automatically. Raw logs are stored by AlienVault for the duration of your subscription. If your subscription expires and you decide not to renew, your AlienVault USM Anywhere instance will be decommissioned 14 days after the expiration. All data, including asset information, orchestration rules, user credentials, events, and vulnerabilities (hot storage), and raw logs (cold storage), will be destroyed.

AlienVault alarm data forwarded to the Cygilant SOCVue platform will be stored for 1 year or until your agreement ends. You then have 30 days to request the data. Cygilant will delete your SOCVue account and purge the associated data 30 days after the agreement ends.

**86. In the event we need comprehensive forensic data for a breach investigation, can you provide it and to what degree?**

Event data in AlienVault hot storage is available for the Cygilant SOC to search and include in reports to assist in a breach investigation. The SOC will assist you with interpreting the data as it relates to the security incident. Raw log data in AlienVault cold storage will no longer be available for the Cygilant SOC team to search, report or provide further analysis on. However, the logs are still available for the customer to download and utilize on their own. This archived data will be provided to the customer in CSV format upon request within 3 business days. Analysis of cold storage data might be possible as an additional professional services engagement depending on availability of SOC resources. Cygilant cannot provide forensic data beyond what was collected as part of the ongoing service. For more comprehensive forensic services, Cygilant can recommend and introduce one of our incident response partners.

## 4.h Pricing

**87. What services from your offerings are being proposed?**

Security Monitoring, Endpoint Management (Detection and Response) and Vulnerability Management

**88. What is the pricing model for each component?**

Cygilant's Security-as-a-Service offerings are subscription-based services licensed to Mayers Memorial Hospital District in the attached pricing proposal. The pricing for our services is an all-encompassing price. There are no one-time costs tied to the contract. All costs are recurring costs and payment is due annually. All technology used (AlienVault USM Anywhere SIEM, SentinelOne,



Qualys and SOCVue platform) to perform Cygilant’s services are included in the overall price of the agreement.

**89. Are additional discount rates available for longer duration contracts? If so, what are they for what duration?**

Yes, the cost/year for Cygilant’s Security-as-a-Service will be discounted on a 3-year agreement (paid annually) as compared to the 1-year agreement attached in this RFP proposal.

**90. Please provide detailed cost breakdowns of your proposal including any additional startup costs, maintenance costs, ongoing support costs, incident retainers and other fees or required payments associated to your solution. If third party software or subscription services are required, include these in this assessment.**

A detailed cost breakdown of our proposal is presented on page 3 of this RFP.

#### 4.i Client Satisfaction

**91. How do you track your customer satisfaction?**

Each of our customers is assigned a dedicated CyberSecurity Advisor (CSA). Your CSA will conduct monthly meetings with your team to go over everything that’s taken place over the last 30 days as well as provide reports to the team. In addition to the CSA, you will be assigned an Account Manager (Sales Representative) and Executive Sponsor (member of our Senior Management Team) to ensure excellence of our services. Customer centricity is very important to our organization, and we strive for excellence.

**92. Do you have SLA’s or SLO’s? If so, please provide the matrix.**

Service desk requests can be initiated by call or email, or by opening a ticket in SOCVue.

The Cygilant SOC will respond to service desk requests based on the priority level of the request as shown in Table 6 below.

Severity	Action	Service Desk Request Targets	Security Monitoring Targets
P1 – Critical	Acknowledgement*	Within 15 minutes	Within 15 minutes
	Response Time**	Within 30 minutes	Within 15 minutes
	Escalation to Manager	Within 2 hours	Within 2 hours
P2 - High	Acknowledgement	Within 30 minutes	Within 30 minutes
	Response Time	Within 1 hour	Within 30 minutes
	Escalation to Manager	Within 4 hours	Within 4 hours
P3 - Medium	Acknowledgement	Within 3 hours	Within 1 hour
	Response Time	Within 6 hours	Within 2 hours
	Escalation to Manager	Within 24 hours	Within 24 hours
P4 - Low	Acknowledgement	Within 8 hours	Within 2 minutes

Severity	Action	Service Desk Request Targets	Security Monitoring Targets
	Response Time	Within 24 hours	Within 4 minutes
	Escalation to Manager	As Required	As Required

Table 1: Service Desk Service Level Agreements

\*Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation. Notification SLAs are subject to low-noise default settings, modified by customer notification preferences.

\*\*Response time is the elapsed time from Acknowledgement to confirmation that a SOC Analyst is investigating the issue.

Cygilant may schedule maintenance outages for Cygilant-owned equipment/servers that are being utilized to perform the services with 24 hours' notice to designated customer contacts. The Service Levels are subject to the following terms, conditions, and limitations:

- The Service Levels shall not apply during scheduled maintenance outages.
- The Service Levels shall not apply in the event of any customer-caused service outage that prohibits or otherwise limits Cygilant from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software by the customer, its employees, agents, or third parties acting on behalf of the customer.

Furthermore, the Service Levels shall not apply to the extent that the customer does not fulfill and comply with the obligations and interdependencies set forth within contractual documents.

### 93. How will breaches of SLA be handled?

When SLA breaches are escalated, Cygilant would perform an RCA (root cause analysis) which would investigate what caused the miss. With that, we would make process or personnel adjustments to prevent reoccurrence.

### 94. Do you ever participate in meetings with clients, regulators and due diligence questionnaires?

Cygilant engages in regular monthly meeting with our clients – as part of the partnership the District and the Cybersecurity Advisor. We are happy to supply necessary information needed for meeting with regulators as well. If the District would need a representative from Cygilant to come on-site for assistance, we are happy to do so as well.

## 5. Cygilant Security-as-a-Service Technical Explanation

### SOCVue Security Monitoring (AlienVault USM Anywhere)

#### Overview:

Cygilant has developed a 24x7 global Security Monitoring service that addresses the significant challenges of security monitoring products:

- Managing the complexity of SIEM and Log Management products
- Lack of trained personnel to manage SIEM and Log Management products
- Difficulty of gaining useful or meaningful information from SIEM and Log Management products

SOCVue® Security Monitoring is a subscription-based service that delivers the proper people, process, and technology for an effective security program. Cygilant Cybersecurity Advisors (CA) will install and manage the AlienVault USM solution, and the Cygilant Security Operations Center (SOC) will continuously monitor and make customers aware of potential security incidents.

The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6).

The key benefits that SOCVue Security Monitoring delivers to customers are:

- Continuous monitoring of log and event data to detect potential security incidents
- Integrated network intrusion detection (IDS), file integrity monitoring (FIM), and threat intelligence feeds
- Timely investigation and notification about incidents that need attention
- Reporting on security events and alerts
- Assistance with compliance needs regarding FFIEC, PCI DSS, HIPAA, and other regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with your Cygilant CA covering the customer's overall security posture and overall system health

#### Key Components of the Service:

An effective security program is made up of People, Process, and Technology. Traditional security monitoring products have focused on the technology aspect without considering how to derive value from the solution. SOCVue Security Monitoring takes a more holistic approach, leading to more actionable intelligence and a proactive security posture.

##### **1. People**

- a. Cygilant Security Operations Center (SOC) – The Cygilant SOC is operational 24x7 and serves as an extension of the customer's own security and IT staff.
- b. Security and Product Expertise – The Cygilant SOC is staffed by information security experts and technicians who are experienced at deploying, managing, and optimizing security monitoring technologies.

- c. Continuous Monitoring – The SOC team provides around-the-clock coverage of the customer’s security environment and will provide timely notification of any security incidents.

## 2. Process

- a. Audit Log Management – The Cygilant SOC helps implement formal process for the Maintenance, Monitoring and Analysis of Audit Logs as recommended by SANS/CIS Critical Security Control #6.
- b. Alert Policies – The SOC team will develop a set of correlation rules that will trigger an alert for suspicious activity or security violations, and they will continuously tune and update policies on an ongoing basis.
- c. Incident Response – The SOC team uses an integrated ticketing system to guide customers through the incident response process from detection to resolution.

## 3. Technology

- a. AlienVault USM – The solution collects, stores, and analyzes security event data from across the IT infrastructure. The solution is cloud-based but may include an on-premises sensor based on your needs.
- b. Managed Solution – Unlike traditional, complicated SIEM solutions, the AlienVault platform is installed, configured, and maintained by the Cygilant SOC team as part of the service.
- c. Cygilant SOCVue® Platform – Manage your incident response process with integrated dashboards, ticketing, and reporting through Cygilant’s custom-built Security Operations and Analytics Platform.

## Service Features:

The Cygilant SOCVue Security Monitoring service provides customers with the following deliverables:

Service	Deliverable
Continuous Security Monitoring & Incident Management	Monitoring of Security Events and Incident Notification <ul style="list-style-type: none"> <li>• Any triggered Alert Policies will be reviewed by Cygilant Security Analysts</li> <li>• Customer will be made aware of potential security threats per the SLA in Section 7</li> <li>• Customer will be provided with possible causes and suggested actions for remediation</li> </ul>
Security & Compliance Reporting	Downloadable Reports <ul style="list-style-type: none"> <li>• Monthly security scorecard reports</li> <li>• Compliance reports for common regulatory frameworks</li> <li>• Custom reports as needed</li> </ul>
Solution Health Review	Regular assessments to ensure proper system performance <ul style="list-style-type: none"> <li>• System resource utilization</li> <li>• Data volume utilization</li> <li>• Event collection statistics</li> <li>• Administration audit logs</li> </ul>
Up to 2 Forensic Log Searches per Month*	Requests for further investigation of an incident * <ul style="list-style-type: none"> <li>• Up to 2 requests per month will be available; not to exceed 2 requests per month</li> <li>• Deliverable: Results/Findings to be provided within 2 business days</li> </ul>
Monthly One-on-One Review Session	Regular 1-hour call with Cygilant Cybersecurity Advisor <ul style="list-style-type: none"> <li>• Review open tickets and incidents</li> <li>• Analyze alert trends</li> <li>• Discuss reporting needs and future deployment plans</li> <li>• Schedule follow-up calls as needed</li> </ul>

## SOCVue Endpoint Management (SentinelOne EDR)

### Overview:

Rooted in 20 years of experience and with hundreds of customers, Cygilant has developed a managed endpoint security service in partnership with SentinelOne that addresses the challenges of preventing, detecting, and responding to attacks – both known and unknown.

#### Key Benefits:

- Improved security posture – Take advantage of SentinelOne’s patented AI algorithms to detect a wide array of threats, plus self-healing response capabilities that reverse malicious activity in real time.
- Dedicated cybersecurity team – Our team of cybersecurity experts work with you for efficient installation and system tuning. You get time back to focus on other priorities.
- Maximize ROI – Cygilant’s affordable Cybersecurity-as-a-Service provides deployment guidance and regular health checks to ensure you are getting the most from your investment.

You can also add 24x7 security operations coverage for your SentinelOne alerts by adding the Cygilant Security Monitoring service to your subscription package.

The Security Monitoring service includes the following benefits:

- Cygilant SOCVue platform – Manage your incident response process with integrated dashboards, ticketing, and reporting through Cygilant’s security operations platform.
- Managed SIEM – Best-of-breed AlienVault solution is installed, configured, and maintained by Cygilant Cybersecurity Advisors.
- Alerts – The SOC develops a set of correlation rules to trigger alerts for suspicious activity or security violations. Rules are fine-tuned, and policies updated to meet your needs.
- Audit log management – Cygilant helps implement the maintenance, monitoring and analysis of audit logs to help meet compliance requirements.
- Security and compliance reporting – Monthly security scorecard reports, scheduled event reports on a daily or weekly basis, automated compliance reports for common regulatory frameworks and custom reports as needed.

Combining log management and security information and event management (SIEM) technology with a 24/7 Security Operations Center (SOC), Cygilant helps you to proactively eliminate threats and meet compliance objectives

## Service Features:

The Cygilant Managed Endpoint Security service provides customers with the following deliverables:

Service	Deliverable
Deployment & Maintenance	<p>Cygilant will deploy and configure the Sentinel One solution.</p> <ul style="list-style-type: none"> <li>• <i>Provisioning of Sentinel One cloud console</i></li> <li>• <i>Assistance with endpoint agent installation</i></li> <li>• <i>Connectivity checks</i></li> <li>• <i>Configuration of initial detection, response, and alerting policies</i></li> </ul>
Threat Review	<p>Cygilant will review with the customer the threats already present in the environment that are discovered during the deployment phase.</p>
Policy Tuning	<p>Cygilant will respond to policy tuning and update requests based on the SLA in section 5.</p> <ul style="list-style-type: none"> <li>• <i>Adding or removing exceptions</i></li> <li>• <i>Modifying automated response policies</i></li> <li>• <i>Tuning alert notification rules</i></li> </ul>
Product Support	<p>Cygilant will respond to product support requests based on the SLA in section 5. Cygilant will be responsible for L1 support handling and may escalate to the SentinelOne support team for L2 support.</p>
Reporting	<p>A Cybersecurity Advisor (CSA) will assist with the configuration of reports including format and scheduling. Requests for ad-hoc reporting can be directed to your CSA.</p>
Monthly Review	<p>Cygilant CSAs will</p> <ul style="list-style-type: none"> <li>• <i>Meet regularly to review the health of the solution, including configurations, reports, and planned changes</i></li> <li>• <i>Work with the customer to ensure ROI and coordinate customer satisfaction activities across Cygilant teams</i></li> </ul>

NOTE: Alert triage and investigation by the Cygilant SOC requires the purchase of *Cygilant Security Monitoring* (a separate service offering).

## SOCVue Unlimited Vulnerability Management (Qualys)

### Overview:

Software flaws or misconfigurations could allow cyber-attackers to gain access to IT systems. These vulnerabilities need to be quickly detected and remediated before they can be exploited.

Cygilant’s SOCVue® Vulnerability Management is a subscription-based service that helps you quickly detect vulnerabilities and provides guidance for remediation. Because it is a managed service, Cygilant handles the deployment and configuration, schedules scans on your behalf, and assists with reporting.

The key benefits delivered by SOCVue Vulnerability Management Service are:

- Regular scanning of IT systems for vulnerabilities to reduce security risk
- Vulnerability reports that provide guidance for reducing your attack surface
- Executive reports to provide summary data for all stakeholders
- SOCVue interface for sorting, filtering, and adding tickets to vulnerabilities
- Monthly meeting with your Cygilant Cybersecurity Advisor to discuss scanning needs and review vulnerability trends

### SOCVue Vulnerability Dashboard:

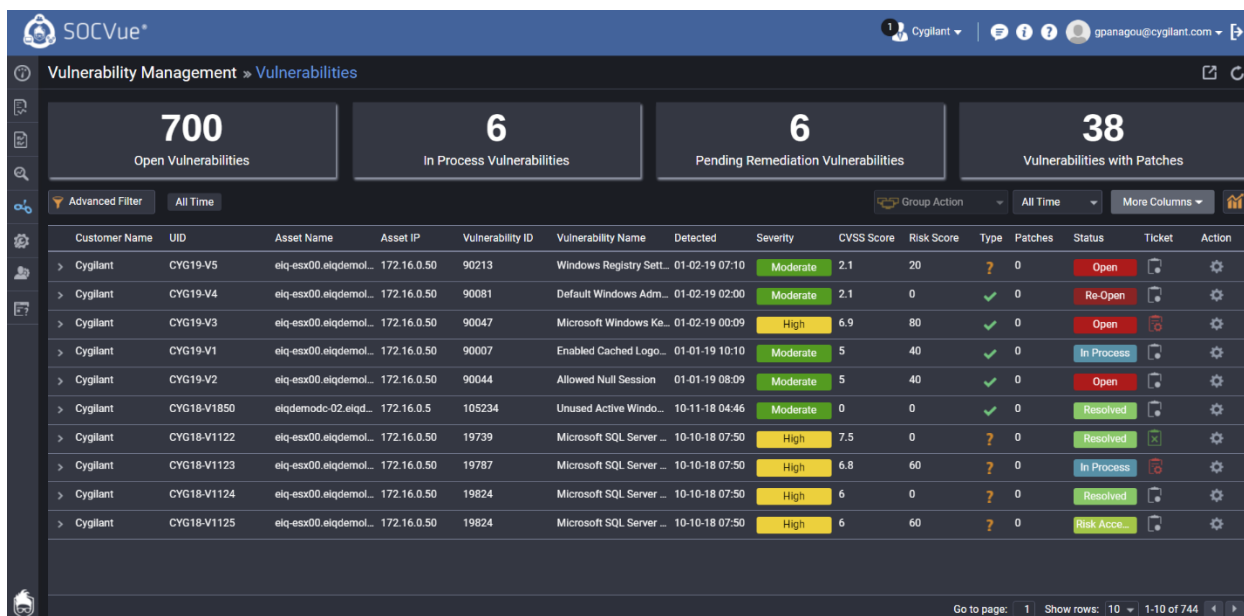


Figure 1: SOCVue Vulnerability Dashboard

### Vulnerability Details

**Vulnerability Name**  
Windows Registry Setting To Globally Prevent Socket Hijacking Missing

<b>Asset Name</b> eiq-esx00.eiqdemolab.com	<b>Asset IP</b> 172.16.0.50	<b>Severity</b> Moderate	<b>Status</b> Open
<b>OS Type</b> Windows 2008 R2 Standard Service Pack 1	<b>Asset Value</b> High	<b>Vulnerability ID</b> 90213	<b>Ticket</b> Not Available

**Scan Results** | Diagnosis | Research | Remediate | Compliance Notes

<b>Last Scan</b> 01-02-19 02:10	<b>Last Detected</b> 01-02-19 07:10	<b>First Detected</b> 01-02-19 07:10	<b>Last Update</b> 01-02-19 03:10
<b>Elapsed Time</b> -946 days, -8 hrs, -19 mins	<b>Asset ID</b> 128117472	<b>Vendor</b> Qualys	<b>Time Zone</b> America/New_York

**Results**

HKLM\SYSTEM\CurrentControlSet\Services\Afd\Parameters DisableAddressSharing is missing.

Export Details to CSV | Close | Ticket Drilldown

Figure 2: SOCVue Vulnerability Details

### Select Status

Status:

- In Process
- In Process
- Pending Remediation
- Pending Validation
- Resolved
- Risk Accepted

Cancel | Change

Figure 3: SOCVue Vulnerability Change Status Workflow



## Service Features:

SOCVue Vulnerability Management service provides customers with the following deliverables:

Service	Deliverable
Vulnerability Assessment	<ul style="list-style-type: none"> <li>• Cygilant will conduct scheduled internal scans of all licensed internal nodes (IP addresses or virtual hosts) using a scanner internal to the network**.</li> <li>• Cygilant will conduct scheduled external scans of all licensed, public IP addresses using a scanner external to the network**.</li> <li>• Vulnerabilities are scored based on exploitability and the business value of the affected system</li> <li>• Customer will be provided with vulnerability description, severity, and recommended actions for remediation.</li> <li>• Customer will be provided with secure access to all information through the SOCVue interface.</li> </ul>
Vulnerability Dashboards & Reporting	<ul style="list-style-type: none"> <li>• Executive Report – providing an overview of current vulnerability status</li> <li>• Detailed Vulnerability Report – all identified vulnerabilities with impact, risk, and recommendations for remediation</li> <li>• SOCVue Scorecards – tracking key remediation metrics and vulnerability trends</li> </ul>
Targeted Vulnerability Scanning	<ul style="list-style-type: none"> <li>• Customer may request an unscheduled vulnerability scan on a targeted system or group of systems</li> <li>• Cygilant will respond to requests as outlined in the SLA in Section 7</li> </ul>
Monthly Review	<ul style="list-style-type: none"> <li>• Regularly scheduled review with Cygilant Cybersecurity Advisor (CSA)</li> <li>• Customer and CSA will discuss vulnerability trends and remediation progress from the previous month</li> <li>• Customer and CSA will outline vulnerability management plans for the coming month</li> </ul>

*\*\*Scans are performed using the Qualys Vulnerability Management (VM) module. Additional Qualys modules are not included. Bring-your-own-license service is available for Qualys VM, Rapid7 InsightVM, and Tenable Nessus. Contact your account executive for details.*

## 6. References

### 6.a Van Buren County Hospital (Keosauqua, IA)

Nate Mahon – IT Manager  
[nathan.mahon@vbch.org](mailto:nathan.mahon@vbch.org)  
(319) 293-3171



---

An Affiliate of **MERCYONE**

### 6.b Fitchburg State University (Fitchburg, MA)

*Sherry Horeanopoulos* – Information Security Officer  
[sah@fitchburgstate.edu](mailto:sah@fitchburgstate.edu)  
(978) 665-3000



### 6.c University Credit Union (Miami, FL)

*Eric Hoskins* – Chief Information Officer  
[ehoskins@ucumiami.org](mailto:ehoskins@ucumiami.org)  
(786) 425-5000



## 7. Additional Information

### 6.a Sample Monthly SOC Report:



# Security Operations Report

August 29, 2020 to September 28, 2020

Summary Report





### Executive Summary

The following report is an account of the Security Operations Center activity during a 30-day period from August 29, 2020 through September 28, 2020. An account of the events, security incidents, and alerts reported is given in numerical and graphical form.

There is currently no OPEN High Severity Security Incidents.

### Incident & Ticket Summary

Incidents Reviewed by  
SOC Analysts

128

Incidents Raised to  
Customer

3

Support Tickets Raised

2

Total Tickets Resolved

4

### Security Incidents raised during reporting period

Subject	Priority	Created Date	SOC Contact	Status
Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon	Medium	09-24-20 16:19	Jon Mendoza	Solved
Privilege Escalation_Potential Zerologon Exploitation	Medium	09-22-20 15:17	Diana Samson	Solved
Account Manipulation_User Account password set to never expire	Low	09-14-20 21:40	Louise Croft	Closed

- CYGAVT-80213-Privilege Escalation\_Potential Exploitation of CVE-2020-1472 Zerologon
  - Alert relates to recognized activity from McAfee Webgateway
  - The SOC are implementing a suppression rule per Gary's request for 'Webgateway' AND EventID =5829
- CYGAVT-80001-Privilege Escalation\_Potential Zerologon Exploitation
  - The SOC investigated and determined it to be a duplication of above
- CYGAVT-80811-Account Manipulation\_User Account password set to never expire
  - User "Hxxxxx" was set to never expire by elowxxxx on 09/14 – Steve confirmed this was an intended action and would be remediated the following day

### Support Tickets Outstanding or Raised During the Reporting Period

Subject	Priority	Created Date	SOC Contact	Status
AlienVault Disconnect - 17th - 21st September	Medium	09-24-20 10:00	Support Team	Solved
Failed login reports	Medium	09-03-20 10:07	Diana Samson	Open

- AlienVault Disconnect - 17th - 21st September
  - Salient account password was set to never expire (security camera machine)
  - Gary confirmed this was expected during an upgrade of the camera system

3

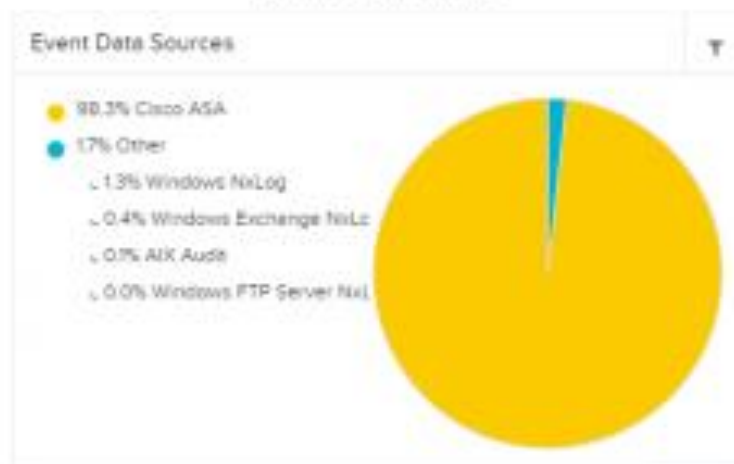


- Failed login reports
  - Appears there was no Audit Policy configured on the Domain Controller which may explain why the logs are not getting to AlienVault
  - Documentation has been provided to Gary for configuration of the Audit Policy and we can retest then

### Event Summary

The following visualizations summarize event data sent to your SIEM solution during the 15-day reporting period (9/13 to 09/28). The first shows what percentage each data source makes up and the second shows the total number of events received over time. There is no alarming spike in events and the dip in numbers occurs during weekends.

Events by Data Source



Events Past 30 Days



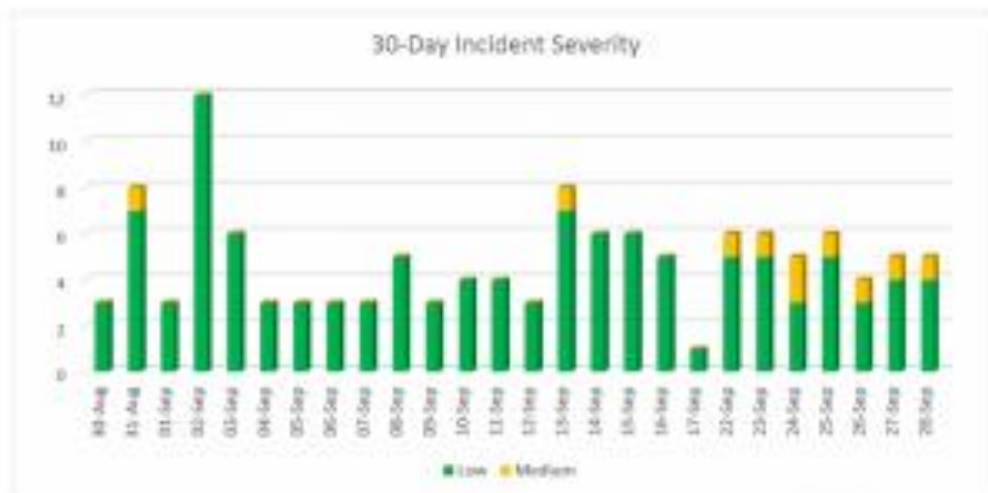


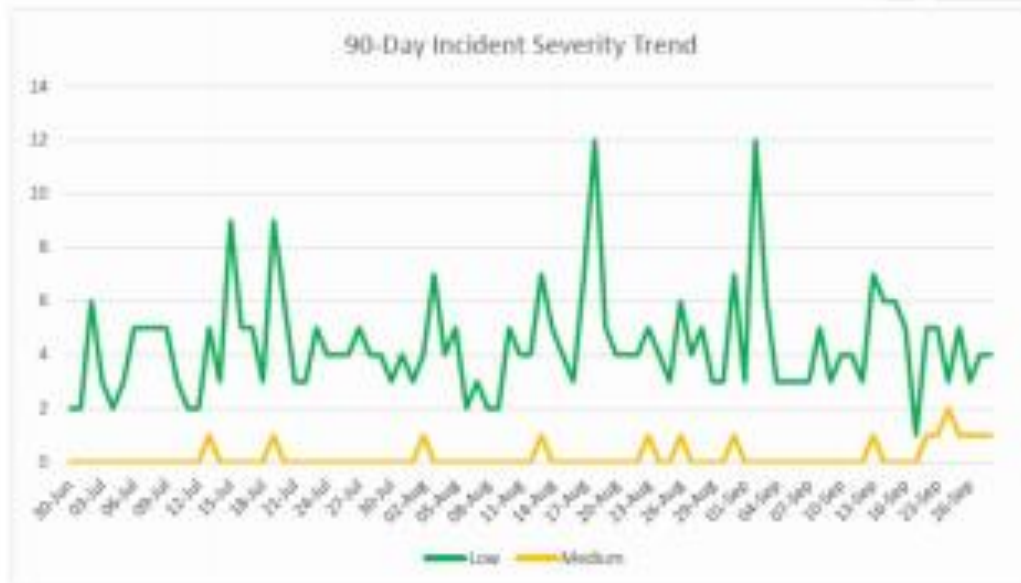
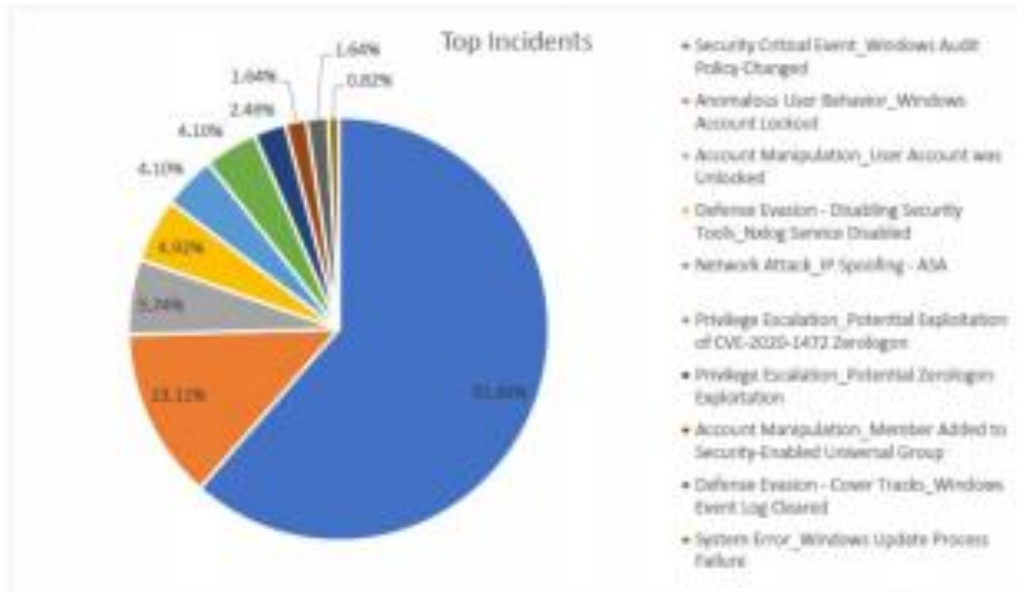
## Incident Summary

The following visualizations show the trend of incidents over a 30-day and 90-day reporting period.

### Highlights & Trends

- Most incidents were low severity, with a total of 118 low severity and 10 medium severity incidents reviewed during the reporting period
  - Low severity incidents
    - Windows Audit Policy Changed – 78
    - Account Lockouts – 15
  - The noisiest day for incidents was 2 Sept with 12 low severity incidents
    - Account lockout – 5, Windows Audit Policy Changed – 3, Member Added to Sec Group – 1, Member Removed from Sec Group – 1, Account Unlocked – 1, IP Spoofing - 1









### Alert Summary

The following table shows the breakdown of alerts triggered in your environment during the reporting period. The table lists out the number of times each alert triggered and is grouped by alert severity.

### Highlights & Trends

- The below details the split of 14 different alerts triggered during the reporting period.
- The majority of alerts were low severity with 78 alerts for **Windows Audit Policy Changed**
  - A full detailed list of the alerts can be found on the accompanying spreadsheet

Alerts Triggered by Severity	
Alert Severity - Alert Name	# of Alerts
<b>High</b>	<b>50</b>
Network Attack_IP Spoofing - ASA	50
<b>Medium</b>	<b>9</b>
Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon	5
Privilege Escalation_Potential Zerologon Exploitation	3
System Error_Windows Update Process Failure	1
<b>Low</b>	<b>118</b>
Security Critical Event_Windows Audit Policy Changed	78
Anomalous User Behavior_Windows Account Lockout	15
Account Manipulation_User Account was Unlocked	7
Defense Evasion - Disabling Security Tools_Nxlog Service Disabled	6
Account Manipulation_Multiple User Accounts Deleted	5
Account Manipulation_Member Added to Security-Enabled Universal Group	2
Defense Evasion - Cover Tracks_Windows Event Log Cleared	2
Account Manipulation_A User Account was Disabled	1
Account Manipulation_Member Removed from Security-Enabled Universal Group	1
Account Manipulation_User Account password set to never expire	1
<b>Grand Total</b>	<b>177</b>

#### Glossary of Terms:

- **Alert** – An event that has triggered a security alarm.
- **Incident** - May be a collection of these events/alerts that SOC/our may aggregate and will be sent to the SOC for review.
- **Security Incident** – An incident that has been raised to the customer for a response, either validation of expected or unexpected behavior. If unexpected, the SOC will investigate further and report back to the customer with a remediation response.

If you have any questions regarding the content of this report, please reach out to your Cyber Security Advisor.

AnnMarie Nayiga-Ramon  
xxxxx@Cygilant.com

7

© 2021 Cygilant. All Rights Reserved. Cygilant, and the Cygilant logo are trademarks or registered trademarks of Cygilant, Inc. in the US and/or other countries. All other product names and/or logos mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.



# MMHD STRATEGIC PLANNING SESSION (CONTINUED)

JULY 28, 2021

# INTRODUCTION

Jeanne Utterback

Louis Ward

# AGENDA

<b>Introduction</b>	<b>Jeanne / Louis</b>	<b>5 Min</b>
<b>Concept &amp; Goal of the Day</b>	<b>Jeanne / Louis</b>	<b>5 Min</b>
<b>June 23 Strategic Session Recap</b>	<b>Louis</b>	<b>5 Min</b>
<b>Revisited Concepts</b>	<b>Louis</b>	<b>20 Min</b>
<b>MRI</b>		
<b>Health Voucher Program</b>		
<b>The Joint Commission (TJC)</b>		
<b>Group Discussion</b>	<b>All</b>	<b>20 Min</b>
<b>Break</b>	<b>All</b>	<b>15 Min</b>
<b>Facilities – Current Timeline &amp; Master Planning</b>	<b>Louis &amp; Ryan</b>	<b>90 Min</b>
<b>Group Discussion</b>		<b>30 Min</b>
<b>Break</b>	<b>All</b>	<b>5 Min</b>
<b>EMR Group Discussion</b>	<b>Louis</b>	<b>30 Min</b>
<b>Next Steps &amp; Wrap Up: Amend Plan or Continue Research?</b>	<b>Jeanne / Louis</b>	<b>15 Min</b>

# CONCEPT & GOAL OF THE DAY

Jeanne Utterback  
& Louis Ward

The purpose of this Strategic Plan is to outline the key strategic objectives that the Board of Directors intends to accomplish by 2025. The Strategic Plan helps provide a link between the Vision and Mission of Mayers Memorial Hospital District to the everyday operational duties of the very hard-working and dedicated staff.

This Plan will outline the strategic objectives, the milestones needed to be achieved to ensure success toward those objectives (success indicators), the risks to the objectives, implementation, monitoring and evaluation.

# RECAP OF JUNE 23

Louis Ward

MRI



# REVISITED CONCEPTS

## Outstanding Patient Services

MRI Analysis	
Rent per day	\$ 3,400.00
Amount of Revenue to pay for the rental	\$ 7,771.99
Amount of Revenue at Care and Cal Zero	\$ 8,947.37
Zero Report Radiology Collection Percentage	44%
Medicare & Medi-Cal Zero %	38%
Approximate amount of procedures to break even	4
Seneca Average	\$ 3,987.09
Eastern Plumas Average Charge	\$ 1,551.70
Mt Shasta Average Charge	\$ 2,553.17
Mercy Redding Average Charge	\$ 4,831.81
Fairchild Average Charge	\$ 3,500.00
Banner Lassen Average Charge	\$ 2,088.46
<b>MAYERS PROPOSED CHARGE</b>	<b>\$2,236.75</b>

MAYERS MEMORIAL  
HEALTHCARE DISTRICT  
*HEALTH VOUCHER  
PROGRAM*

# Health Voucher Program

## Heath Districts can offer voucher (coupons) to the District's tax payers

### **1. Modoc Medical Center**

A voucher booklet valued at \$150 can be picked up from the Last Frontier Healthcare District office annually

MMC allows the vouchers to be used to offset copays in the clinic, lab costs, emergency room costs, and imaging costs. The vouchers reduce the out of pocket costs of the patient after insurance has paid.

### **2. Southern Humboldt Healthcare District**

A very similar program exists at SHHD providing their citizens a booklet values at \$125.

## Benefits of the voucher program:

- 1. Increase utilization of services**
- 2. Tax payers feel more value when paying annual taxes**
- 3. Patient loyalty**

## How this might work here

**MMHD has 3,495 unique property/parcel owners in the district.**

1. We have a special assessment tax that considers the assessed value of the property rather than a flat parcel tax
2. We could provide a booklet valued at \$100
3. Policies and Education of staff would be necessary
4. Community Education would be necessary.

# THE JOINT COMMISSION

# The Joint Commission (TJC)

## 10 Steps for Joint Commission Accreditation

1. ~~Learn about working with TJC~~
2. ~~Review requirements~~
3. Assess our readiness
4. Apply for accreditation
5. Prepare for our onsite survey
6. Address any identified gap areas
7. Participate in our first TJC survey
8. Complete any post survey follow up activities
9. Celebrate/publicize our accomplishment
10. Maintain survey readiness

The first two steps have been taken – we have checklists and tracer questions and all kinds of TJC supporting materials that will help us on our next step of assessing readiness.

\*There is an attached white paper that details this process more specifically.

## Cost for TJC:

Assuming 3 surveyors for a 3 day survey (commonly what we see from the state)

**Annual fee:** \$2,850

### **Triannual survey fees:**

\$2790/surveyor for Day 1 = \$8,370

\$1465/ surveyor for every subsequent day = \$8790 for the next 2 days

**Total for survey year:** \$17,160 + \$2,850 = \$20,010 (plus expenses for the survey team (TBD) around \$556/month.

## All we have to do is meet the mark and stay TJC survey ready:

Using our LEAN framework for improvement and TJC focused department level dashboards we can integrate this into our QAPI plan for the district and maintain readiness.

# GROUP DISCUSSION

BREAK - 15 MIN

# REVISITED CONCEPTS

## FACILITIES



# REVISITED CONCEPTS

## Outstanding Facilities

Open gym facilities for employees

Bigger and comfortable employee's dining area

Kitchen redoing

Garden with walking areas for use of residents and staff

Clinic in Fall River

Replace the old building with new ones - acute and cafeteria

FACILITIES

CURRENT TIMELINE &  
MASTER PLANNING

# FACILITIES TIMELINE

2021
Demolition of 1956 Buildings
Design PT and Cardiac Rehab gym
Design Storage Plan
2022
Construct PT & Cardiac Rehab gym
Design Fall River Clinic Space
Construct Storage Plan
2023
Construct Fall River Clinic
Construct SNF Refresh

## *Outstanding Facilities Timeline*

2024-2026
Design and permitting for Facility Master Plan: includes new Acute space, Kitchen, Cafeteria, HVAC Updates
2026-2028
Construction of Facility Master Plan

# Master Facility Planning



**Mayers Memorial  
Hospital District**  
*Always Caring. Always Here.*

# Option 1

- Renovate existing hospital spaces to be compliant with SPC & NPC standards
- Remove Acute Care Services from Surgery Department

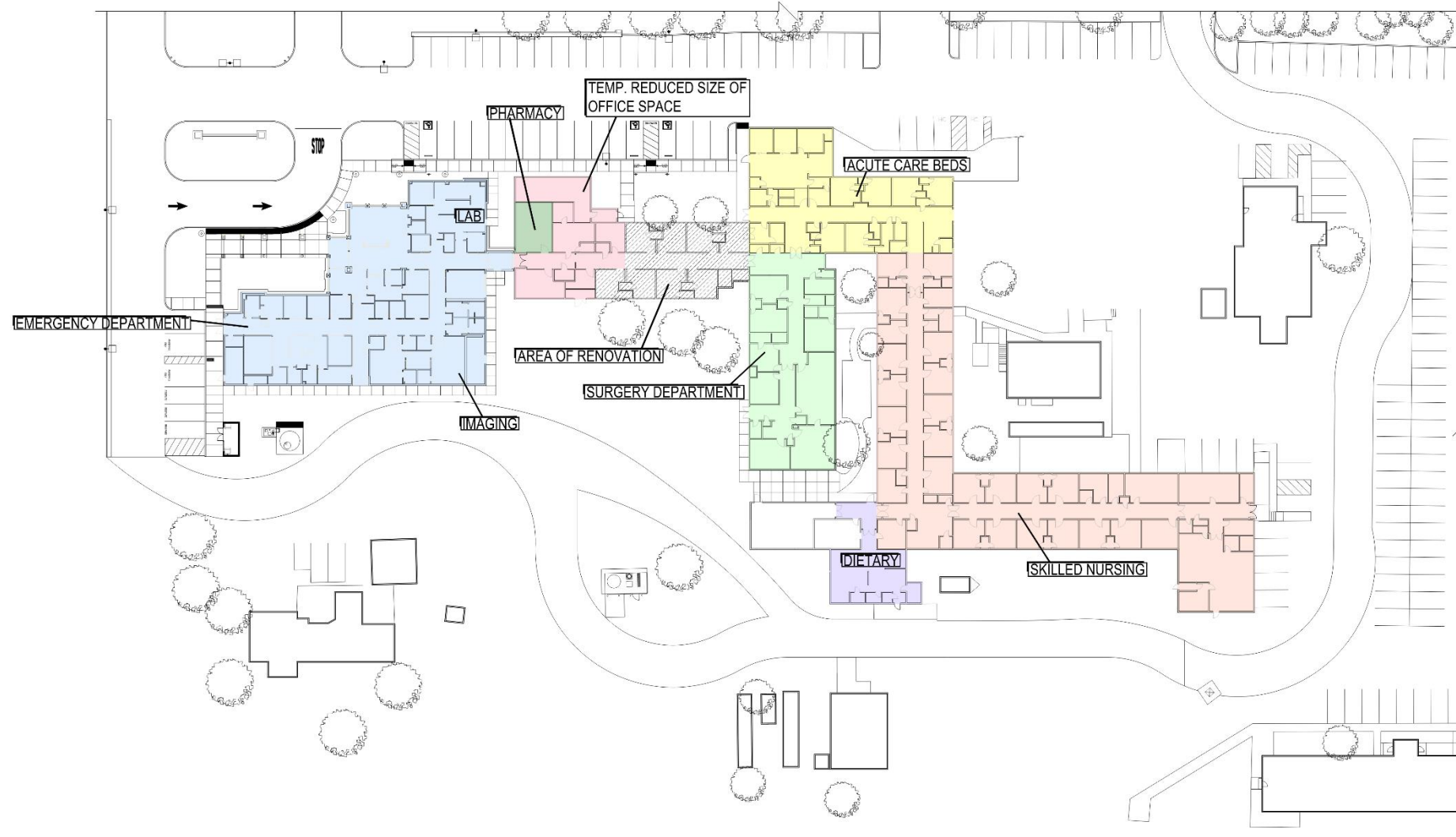
Existing Hospital Site



LEGEND					
	EMERGENCY DEPARTMENT		ACUTE CARE BEDS		PHARMACY
	SURGERY DEPARTMENT		DIETARY		
	OFFICES		SKILLED NURSING		

EXISTING OVERALL HOSPITAL PLAN 1





- Renovate portion of existing office space to accommodate temp. acute care beds.

LEGEND					
	EMERGENCY DEPARTMENT		ACUTE CARE BEDS		PHARMACY
	SURGERY DEPARTMENT		DIETARY		AREA OF RENOVATION
	OFFICES		SKILLED NURSING		

↑ OPT. 1 - PHASE 1 OVERALL HOSPITAL PLAN 1





- Move acute care beds to renovated office space
- Renovate existing acute care bed space to be NPC & SPC compliant

LEGEND			
	EMERGENCY DEPARTMENT		PHARMACY
	LAB		AREA OF RENOVATION
	ACUTE CARE BEDS		DIETARY
	SURGERY DEPARTMENT		SKILLED NURSING
	OFFICES		

↑ OPT. 1 - PHASE 2 OVERALL HOSPITAL PLAN 1



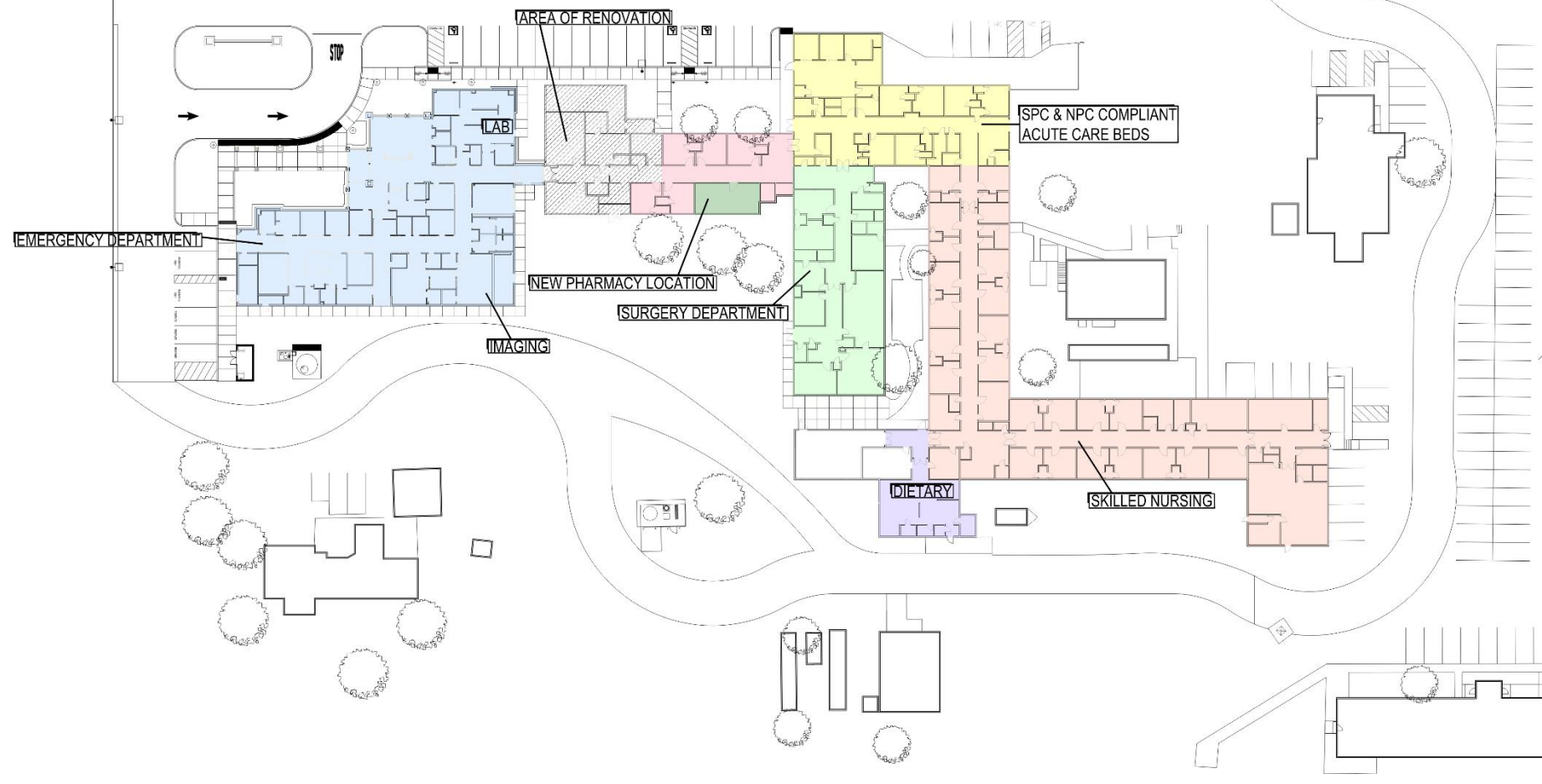




- Move acute care beds back to renovated space.
- Renovate office space used for the temp. acute care beds to a new pharmacy/office space
- Redirect hallway so path of travel is no longer through the surgery department

LEGEND		
<span style="background-color: #ADD8E6; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> EMERGENCY DEPARTMENT	<span style="background-color: #FFFF00; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> ACUTE CARE BEDS	<span style="background-color: #90EE90; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> PHARMACY
<span style="background-color: #90EE90; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> SURGERY DEPARTMENT	<span style="background-color: #DDA0DD; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> DIETARY	<span style="background-color: #FFB6C1; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> AREA OF RENOVATION
<span style="background-color: #FFB6C1; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> OFFICES	<span style="background-color: #FFDAB9; border: 1px solid black; display: inline-block; width: 15px; height: 10px;"></span> SKILLED NURSING	





- Remodel rest of existing office and pharmacy space

LEGEND		
EMERGENCY DEPARTMENT	ACUTE CARE BEDS	PHARMACY
SURGERY DEPARTMENT	DIETARY	AREA OF RENOVATION
OFFICES	SKILLED NURSING	

OPT. 1 - PHASE 4 OVERALL HOSPITAL PLAN 1





- Remove surgery department from acute care services and repurpose as out patient only.
- Remove building surgery department is located in from OSHPD jurisdiction

LEGEND		
<span style="color: blue;">■</span> EMERGENCY DEPARTMENT	<span style="color: yellow;">■</span> ACUTE CARE BEDS	<span style="color: green;">■</span> PHARMACY
<span style="color: lightgreen;">■</span> SURGERY DEPARTMENT	<span style="color: lightblue;">■</span> DIETARY	<span style="color: hatched;">■</span> REMOVAL OF ACUTE CARE SERVICES & FROM OSHPD JURISDICTION
<span style="color: pink;">■</span> OFFICES	<span style="color: peachpuff;">■</span> SKILLED NURSING	

OPT. 1 - PHASE 5 OVERALL HOSPITAL PLAN 1



## Option 2

- Addition of new NCP & SPC compliant building
- Removal of existing office area, acute care beds, surgery department and skilled nursing departments from OSHPD jurisdiction



- Existing Hospital Site

LEGEND

EMERGENCY DEPARTMENT	ACUTE CARE BEDS	PHARMACY
SURGERY DEPARTMENT	DIETARY	
OFFICES	SKILLED NURSING	

↑ EXISTING OVERALL HOSPITAL PLAN 1



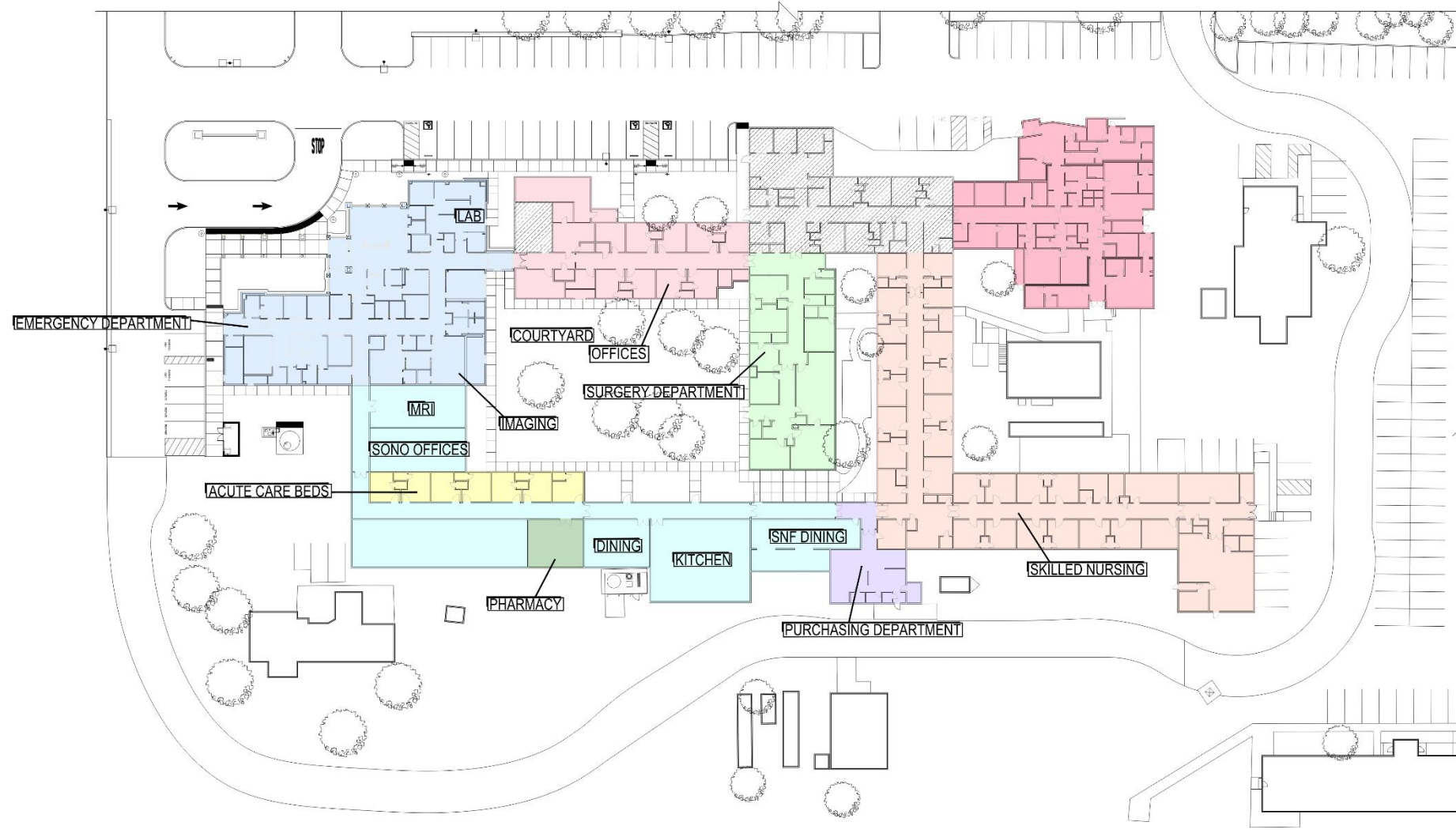


Site demolition work where the new building will be located

LEGEND					
	EMERGENCY DEPARTMENT		ACUTE CARE BEDS		PHARMACY
	SURGERY DEPARTMENT		DIETARY		
	OFFICES		SKILLED NURSING		

↑ OPT. 2 - PHASE 1 OVERALL HOSPITAL PLAN 1





- Addition of new NPC & SPC compliant building
- New courtyard created between buildings

LEGEND					
	EMERGENCY DEPARTMENT		ACUTE CARE BEDS		PHARMACY
	SURGERY DEPARTMENT		PURCHASING		NEW ADDITIONS
	OFFICES		SKILLED NURSING		DEPARTMENTS TO BE RELOCATED

↑ OPT. 2 - PHASE 2 OVERALL HOSPITAL PLAN 1  
SCALE: 1" = 20'

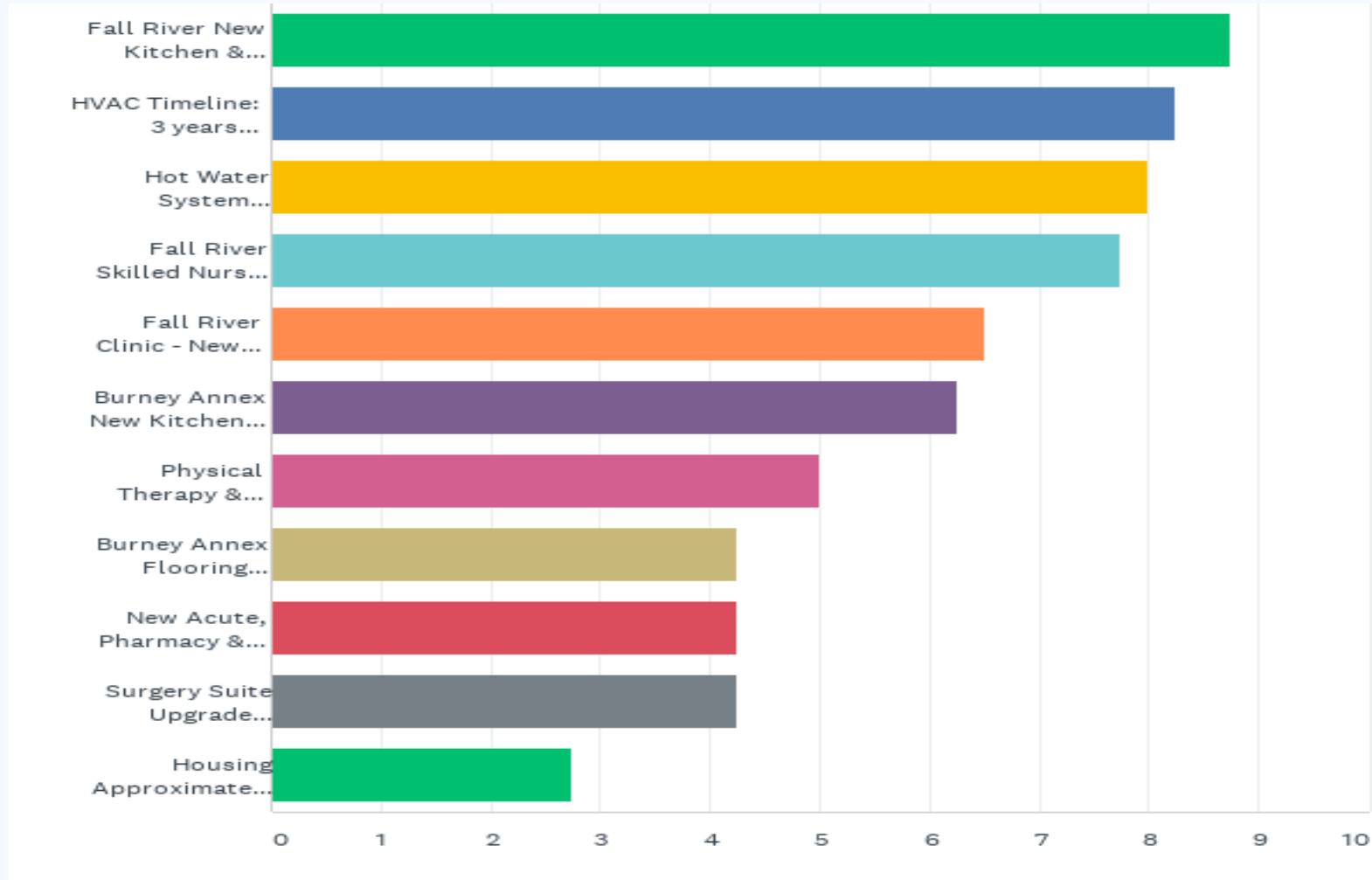


FACILITIES

SURVEY RESULTS OF BOD  
PROJECT PRIORITIZATION



# BOD Prioritization of Facility Projects – Survey Monkey Results



# BOD Prioritization of Facility Projects – Survey Monkey Results

Facility Projects	1	2	3	4	5	6	7	8	9	10	11	Total	Score
Fall River New Kitchen & Dining Timeline: 2 Years Approximate Project Cost: \$3,000,000	50%	0%	0%	25%	0%	0%	25%	0%	0%	0%	0%	4	8.75
HVAC Timeline: 3 years Approximate Project Cost: \$2,600,000	0%	0%	75%	0%	0%	25%	0%	0%	0%	0%	0%	4	8.25
Hot Water System Timeline: 1 Year Approximate Project Cost: \$500,000	0%	75%	0%	0%	0%	0%	0%	0%	0%	25%	0%	4	8
Fall River Skilled Nursing Upgrades Timeline: 18 Months Approximate Project Cost: \$300,000	25%	0%	0%	25%	0%	50%	0%	0%	0%	0%	0%	4	7.75
Fall River Clinic - New Build Timeline: 2 Years Approximate Project Cost: \$4,000,000	25%	25%	0%	0%	0%	0%	0%	25%	0%	0%	25%	4	6.5
Burney Annex New Kitchen Timeline: 2 Years Approximate Project Cost: \$1,500,000	0%	0%	0%	25%	25%	25%	0%	25%	0%	0%	0%	4	6.25
Physical Therapy & Cardiac Rehab Timeline: 2 Years Approximate Project Cost: \$2,600,000	0%	0%	25%	0%	0%	0%	0%	50%	25%	0%	0%	4	5
Burney Annex Flooring Project Timeline: 6 Months Approximate Project Cost: \$200,000	0%	0%	0%	0%	50%	0%	0%	0%	0%	25%	25%	4	4.25
New Acute, Pharmacy & Ultrasound Space Timeline: 3.5 Years Approximate Project Cost: \$11,000,000	0%	0%	0%	0%	25%	0%	25%	0%	25%	25%	0%	4	4.25
Surgery Suite Upgrade Timeline: 1 Year Approximate Project Cost: \$500,000	0%	0%	0%	25%	0%	0%	25%	0%	25%	0%	25%	4	4.25
Housing Approximate Timeline: 2 Years Approximate Project Cost: \$500,00 to \$1,000,000	0%	0%	0%	0%	0%	0%	25%	0%	25%	25%	25%	4	2.75
												Answered	4

# GROUP DISCUSSION

BREAK - 5 MIN

# EMR GROUP DISCUSSION

# EMR



*A driving force for health equity*



Rough Budget	
EPIC system and Installation	\$ 1,200,000.00
Interim Onsite Project Manager	\$ 200,000.00
Hardware	\$ 150,000.00
Data Migration	\$ 100,000.00
New Accounting/Purchasing/HR Software	\$ 125,000.00
Buyout of current software contract	\$ 140,000.00
Interfaces	\$ 125,000.00
Total	\$ 2,040,000.00

NEXT STEPS:  
AMEND PLAN OR  
CONTINUE  
RESEARCH?  
AND WRAP UP

Jeanne Utterback

Louis Ward

Chief Executive Officer  
Louis Ward, MHA



Mayers Memorial Hospital District

**Board of Directors**  
Jeanne Utterback, President  
Beatriz Vasquez, Ph.D., Vice President  
Tom Guyn, MD, Secretary  
Abe Hathaway, Treasurer  
Tami Vestal-Humphry, Director

Board of Directors  
**Quality Committee**  
**Minutes**

August 11, 2021 @ 1:00 PM  
Fully Remote Zoom Meeting

*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	<b>CALL MEETING TO ORDER:</b> Board Chair Jeanne Utterback called the meeting to order at 1:01 pm on the above date.			
	<b>BOARD MEMBERS PRESENT:</b>		<b>STAFF PRESENT:</b>	
	Jeanne Utterback, President Tom Guyn, MD., Secretary		Ryan Harris, COO Candy Detchon, CNO (in ER) Jack Hathaway, Director of Quality Dawn Jacobson, Infection Preventionist Alex Johnson, Facilities Manager Ryan Nicholls, IT Manager Jennifer Levings, Data Analyst Jessica DeCoito, Board Clerk	
	<b>ABSENT:</b> Louis Ward, CEO Laura Beyer Sherry Yochum, Housekeeping Manager Susan Garcia, Dietary Manager Delaney Harr, Purchasing Manager			
	<b>Community Members Present:</b>			
2	<b>CALL FOR REQUEST FROM THE AUDIENCE – PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS</b>			
	None			
3	<b>APPROVAL OF MINUTES</b>			
	3.1	A motion/second carried; committee members accepted the minutes of July 14, 2021.	<b>Guyn, Hathaway</b>	<b>Guyn – Y Utterback – Y</b>
4	<b>REPORTS: QUALITY PATIENT SERVICES</b>			
	4.1	<b>IT:</b> Received our security report from Bansec. We have improved from below average security rating to average ratings. And have already made adjustments to be more secure.		
	4.2	<b>Purchasing:</b> Obvious how the departments are going to be integrated into the Purchasing department to meet everyone's needs. Great Team Work!		
	4.3	<b>Dietary:</b> Worry some that we are short staffed. But thankful we have a great environment that allows others in the		
	4.4	<b>SNF Events/Survey:</b> still within the survey window. Keeping up on making sure all of the areas of concern in both mock surveys for SNF and Acute, are being addressed. Working on three different orders – one that does not have an AFL (all facilities letter attached). Today we released patient and resident visitor restrictions. Information is being communicated with patients, residents and families.		
	4.5	<b>Infection Control:</b> vaccine rate has gone up to 71%. Lindsey has started school to finish her path to becoming an RN. We have had a few COVID cases both of vaccinated and non-vaccinated individuals. We have added vaccination status onto the triage screening to help us identify quicker.		



5	<b>REPORTS: QUALITY STAFF</b>	
	5.1	<b>Environmental Services:</b> working on some options to help recruit and retain staff.
	5.2	<b>Safety:</b> Great job on the trainings.
6	<b>REPORTS: QUALITY FACILITIES</b>	
	6.1	<b>Maintenance:</b> trying to fill for some open positions. Completing the install of the microbiology hood today. Then testing will begin and certification needs to be completed before we can put it into use. Hot water heaters and HVAC units will be in the same project but are different scopes of work. All three major projects just added to the Strategic Plan can be going on at the same time. This makes the project bigger which could attract a lot more contractors to bid and will be easier for permitting and OSHPD approvals if it's under one project versus three. Great job on the exterior work being done on the facilities and especially the gazebos out back for employees and residents.
7	<b>DIRECTOR OF QUALITY</b>	
	7.1	<b>Director of Quality Update:</b> finishing up the electronic reporting platform – Zendesk. Once this process is complete, then we can launch it on our website and start receiving the complaints from patients. And then begin to track the issues, create solutions. Nursing Training Program feedback was received and we are working on a plan of corrections and responses to get back by Friday, August 13 <sup>th</sup> . LEAN projects picking back up. One project includes a time study for breakfast and dinner staffing and getting the meals out to residents in an appropriate time. Diet Order Process has also been a project identified that deserves a LEAN method applied to it. Prime project reports due on August 24 <sup>th</sup> with tracking of Obesity.
	7.2	<b>CMS Core Measures:</b> received quotes from outside companies for data analysis and they were much larger than what is desired. Finding a program that helps navigate all the data and what is valid vs not, but not every program provides the same.
	7.3	<b>5-Star Rating:</b> still working on getting that 5 <sup>th</sup> star.
8	<b>OTHER INFORMATION/ANNOUNCEMENTS:</b> CEO to provide vaccination percentage update in his weekly update to BOD. Pam to manage the Quality Committee Meetings while Jessica is out on maternity leave.	
9	<b>ADJOURNMENT: at 1:54 pm</b> Next Regular Meeting – September 8, 2021	

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](http://www.mayersmemorial.com).



# Mayers Memorial Hospital District

*Always Caring. Always Here.*

**Executive Director of Community Relations & Business Development – Valerie Lakey**  
**August 2021 Board Report**

## **Legislation/Advocacy**

The state legislature is back from recess and have a lot of work to do before session ends September 10th. The two major items are still on the table. There is a lot of opposition from labor and CNA regarding the Disaster Preparedness/Seismic proposal. If this is successful, it will allow for an extension to 2037 and focus on the emergency services portion of hospitals.

### **Disaster Preparedness/Hospital Seismic Mandate**

The administration has moved forward, as part of budget conversations, a proposal to refocus and extend the 2030 hospital seismic mandate.

### **Office of Health Care Affordability**

Conversations continued regarding the Office of Health Care Affordability during the summer recess. The Legislature, working with the administration, will be taking up the issue up when it the issue, and it will likely be part of continuing budget discussions.

We will follow these items and several other bills as the session winds down. Regular contact with legislators and advocacy letters are top priority.

## **Marketing/Public Relations/Recruiting**

We have been very busy in marketing and public relations. We are excited about the launch of the new commercial and “Easy” campaign. We will be using the theme in our upcoming booth at the Inter-Mountain Fair. Initial reports are showing great response and increased web activity from the ads. The ads along with some print materials, Mayers “branded” content on lobby televisions and new website features are all designed to show the continuity of care within our facility, clinic and other services. Here is an overview of some of the recent stats:

### **KRCR Website ads**

As a part of our KRCR/KCVU package, we have digital ads on the news website. These all link to our webpage. We can have as many different ads as we want. For now we are featuring the clinic, pharmacy, telemedicine and ease of access to care.

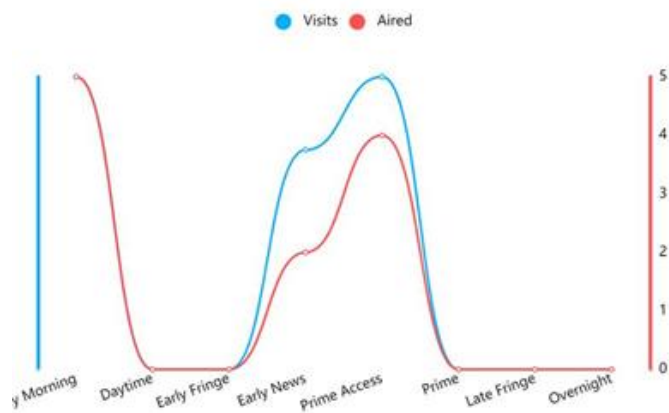
45077 - Mayer Memorial Hospital - Banner Ads - 300x250 - Jul 2021 ID: 138356808293   300x250   Third party	Jul 20, 2021 10:03 AM   EDT	Aug 1, 2021 2:59 AM   EDT	12,338	4	0.03%
45077 - Mayer Memorial Hospital - Pharmacy - Banner Ads - 300x250 - Jul 2021 ID: 138356843847   300x250   Third party	Jul 20, 2021 10:00 AM   EDT	Aug 1, 2021 2:59 AM   EDT	12,353	1	0.01%
45077 - Mayer Memorial Hospital - Mask - Banner Ads - 300x250 - Jul 2021 ID: 138356841732   300x250   Third party	Jul 20, 2021 9:59 AM   EDT	Aug 1, 2021 2:59 AM   EDT	12,638	7	0.06%
45077 - Mayer Memorial Hospital - Clinic - Banner Ads - 300x250 - Jul 2021 ID: 138356843208   300x250   Third party	Jul 20, 2021 9:57 AM   EDT	Aug 1, 2021 2:59 AM   EDT	12,671	2	0.02%



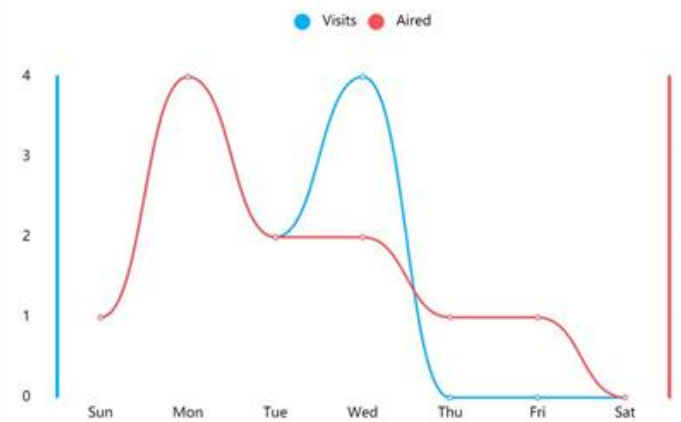
See below for a sample of television commercials aired versus website visits during air time. The commercial airs on KRCR (ABC) and KCVU (Fox)

## KRCR

Performance By Daypart



Performance By Day Of Week



### Top Visits By Station

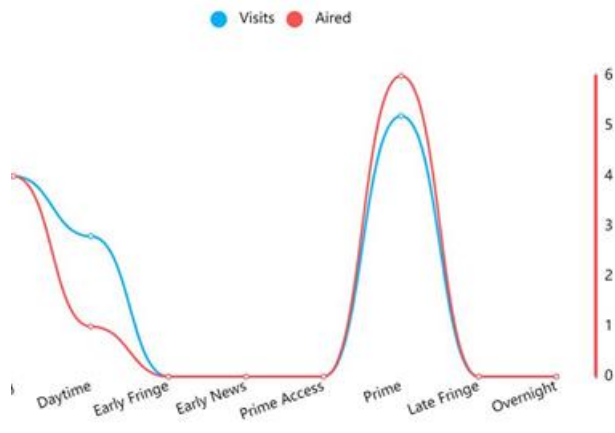
Stations	Visits	Times Aired
KRCR	11	11

### Web Visits By Hour Of Day

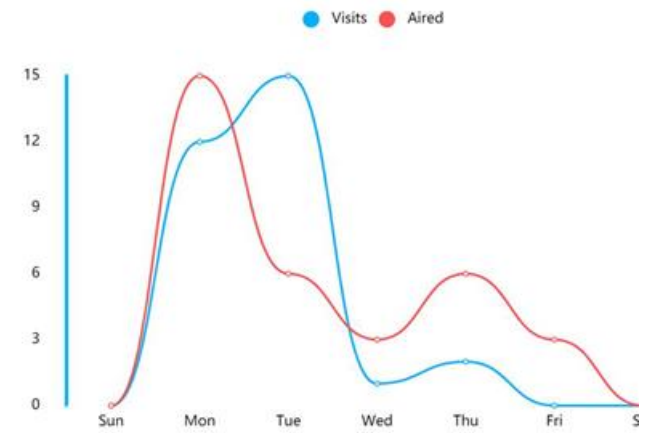
Hour	Visits	Times Aired
5am	1	2
6am	3	3
5pm	3	2
7pm	4	4

## KCVU

### Performance By Daypart



### Performance By Day Of Week



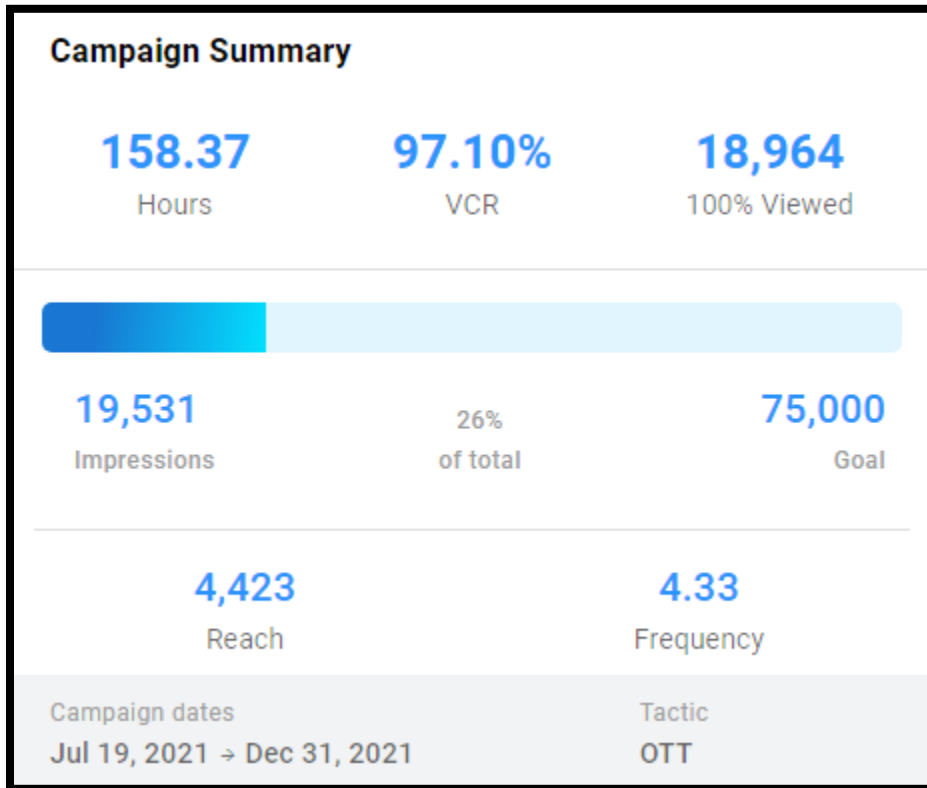
### Top Visits By Station

Stations	Visits	Times Aired
KCVU	30	11

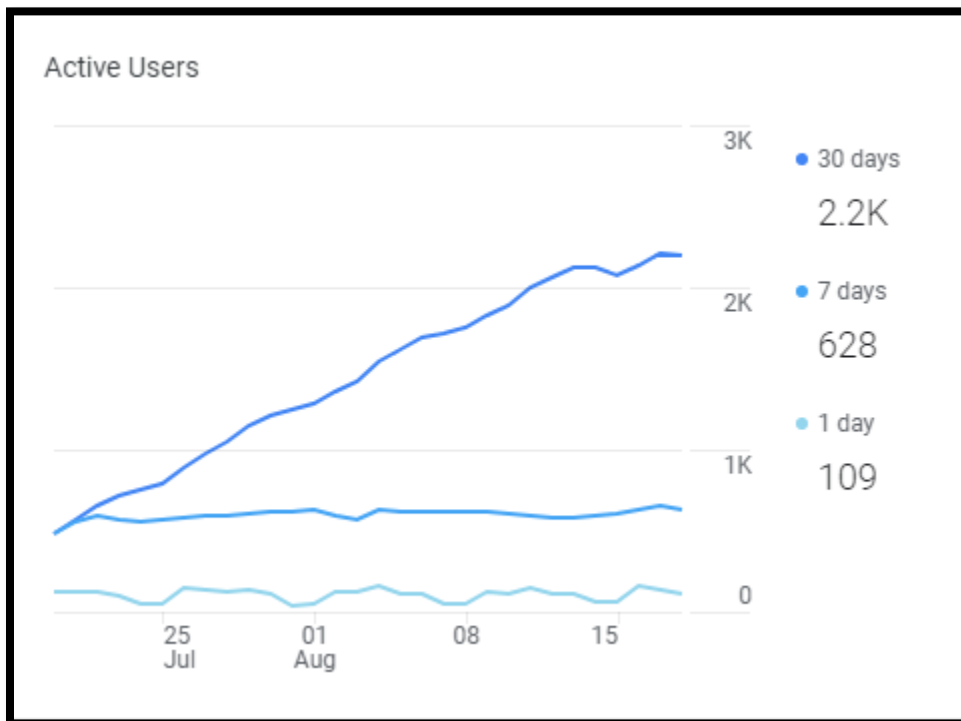
### Web Visits By Hour Of Day

Hour	Visits	Times Aired
10pm	13	6
7am	10	3
9am	7	1
6am	0	1

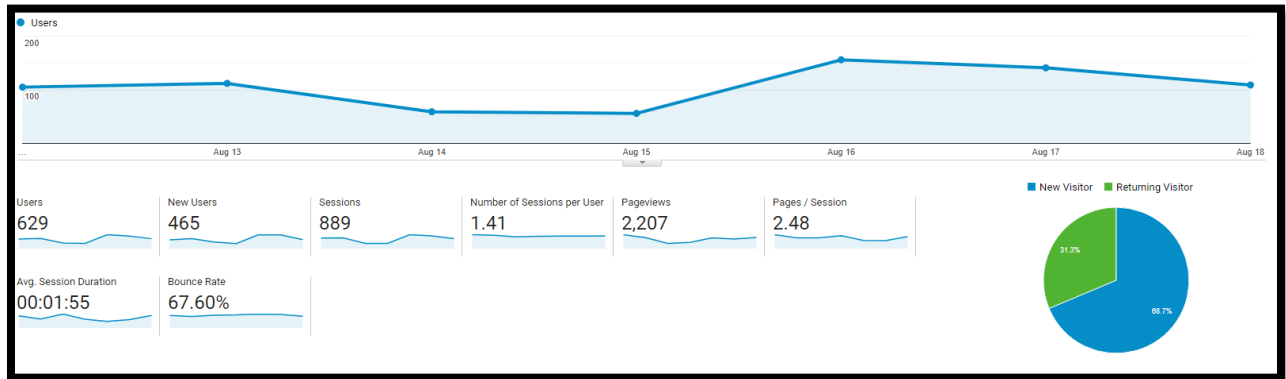
Our 30 second spot is also placed on On-Dmeand television (Hulu, Sling and many others)



Here is a snapshot of Website Activity – you can clearly see increased website visits.



## Google Analytics August 12 – 18, 2021 – Website User Report



### Fair Booth

Our collaborative booth with the foundation is coming along nicely. We are also Fair Sponsor again this year. Be sure to sign up to “man” the booth!

### Disaster/Emergency Preparedness/Safety – Safety report is also provided this month

For the month of August are focusing on CODE GREEN - Evacuations. Again, we have been providing education materials, quizzes and mock drills all related to the CODE.

### This information is worth resending:

We are emphasizing to staff the importance of “knowing what you need to know before you need to know it”. We have provided many resources and are encouraging staff to be familiar with processes and where to go for emergency information and resources. (See links below)

- [Emergency Things to Know](#)
- [MMHD Code Binder](#)
- [Emergency Contact List](#)
- [Disaster Call Tree](#)
- [My EOP App](#)

We have also been providing resources for [Survey Readiness](#)



## Operations Report August 2021

Statistics	July YTD FY22 <i>(current)</i>	July YTD FY21 <i>(prior)</i>	July Budget YTD FY21
Surgeries <i>(incl. C-sections)</i>	2	7	8
➤ Inpatient	0	0	2
➤ Outpatient	2	7	6
Procedures <i>(surgery suite)</i>	10	13	16
Inpatient	182	62	89
Emergency Room	387	354	417
Skilled Nursing Days	2432	2473	2330
OP Visits (OP/Lab/X-ray)	1396	1021	1101
Hospice Patient Days	162	86	161
PT	231	258	212

\*Note: numbers in RED denote a value that was less than the previous year.

### **Chief Clinical Officer Report**

**Prepared by: Keith Earnest, CCO**

Verbal report will be given at the meeting.

### **Chief Nursing Officer Report**

**Prepared by: Candy Vculek, CNO**

COVID has once again become a significant issue and there have been a number of new Public Health Orders with associated AFL's from CDPH that are requiring changes in hospital processes.

- Visitors are required to provide either proof of vaccination or a negative COVID test within 72 hours. This order is in effect for both the long term and acute care units. MMHD will provide a COVID test to any visitor wishing to enter who needs a test. The screening has already prevented visitors who tested positive from entering the facility. This order is in effect.
- Non-vaccinated employees will be required to test twice weekly and wear N-95 level masks. This order goes into effect August 23<sup>rd</sup>. MMHD has already been requiring the non-vaccinated employees to wear N-95 masks.
- Mandatory COVID vaccination order was also issued by CDPH. This order is set to take effect September 30<sup>th</sup>. There are no clear enforcement guidelines associated with this order.

### ***COVID Unit***

- Plans are in place to re-open the 4-bed COVID unit. Several COVID positive patients have been admitted this week due to inability to transfer them to another facility.

### **Staffing**

- Station 1 is fully staffed. Several employees are just finishing orientation.
- Emergency Department continues to have three (3) vacancies. Travelers are filling this position so the department is staffed.
- SNF has 20 vacant C.N.A positions which is a decrease from 24 vacancies in the prior month. Nursing positions on the SNF are much better. At present, there are two vacant LVN positions and one vacant RN spot.
- At present, there are several “extra” registry nurses that are being kept on staff. This is to cover the need for nurses to work the COVID unit.
- The next Shasta College C.N.A. class starts this week and MMHD has FOUR (4) students enrolled. There have been delays in obtaining approval from CDPH for the internal C.N.A. program. MMHD continues to work towards approval and hope to get the program operational by the first of the year.

### ***SNF Report***

- SNF director is submitting report separately for quarterly board report.
- Activities
  - Numerous special activities were held this summer for the residents in addition to the daily scheduled events. Fishing trips, vegetable and flower gardens at both facilities, picnics, afternoon drives to look at the valley, and restaurant dining trips are just a few of the events.
  - The activity aides are now working 12-hour shifts and providing activities after supper. This increases the amount of staff in the evenings, which decreases falls as well as enhancing the quality of life for the residents. Nursing has commented on the positive aspects of the change.
  - Staffing for the Activity Department can be difficult. It is an entry-level position and some staff tend to move through the department quickly. At present, there are two vacant positions.

### ***Acute Care Report***

- June Acute ADC .63, Swing ADC; .3.6, LOS 12, OBS days: 7.84.
- FTE: RN's 7, includes Acute Asst. Mgr. Per diem: RN's 3. LVN-1. RN Traveler-1(contract expires end of Aug), RN Registry-2 (will maintain for COVID surge). FT CNA's: 4, 1 on LOA. 2-FT RN's on orientation to be complete by end of August.
- The acute care unit has been very busy for the past two months. Part of the increased census is related to the on-boarding of a new Emergency Department physician who more effectively utilizes our inpatient beds.

### ***Outpatient Surgery***

- The nursing director is building a plan with Modoc Medical Center to begin an orientation program for a new OR circulator that has been orienting in the pre/post area. She will train between our facility and Modoc.
- The current surgery scrub tech has moved to different department. The position is posted with one remaining part-time Scrub Tech in department.
- CRNA coverage is in place through November.



### ***Outpatient Medical Unit***

- The Outpatient Medical Unit was returned to its former space within the past two months. The need to provide an isolation area for COVID positive patients means OPM will be relocating to the Station 3 hallway. This department should be commended for their flexibility in these difficult times as we have moved them numerous times.

### ***Emergency Department***

- The Emergency Department treated 377 patients in July.
  - 34 arrived by ambulance
  - 16 transferred to higher level of care
  - 21 admitted to acute care, in the month of July.
- ED transfers continue to be problematic. All the hospitals are experiencing staffing shortages as well as increased census. Patients continue to be transferred over a much larger geographic distance, and are taking increasing long periods of time to be transferred.

### ***Laboratory***

- PCC Interface –
  - We are currently awaiting Point Click Care's (PCC) approval on the interface work we have been doing with PCC. Once PCC approves the work, we can select a go live date and begin to get our lab results for SNF residents directly into their charts. This will be very helpful for staff in the SNF as all the information regarding labs will be easily assessable and will no longer require accessing a separate EHR for results.
- Microbiology
  - The hood is almost done! The connection is within 6 inches now – just one more piece and we will have micro back in house. Adding revenue and benefit to the hospital and community respectively.
- LEAN process improvement plans
  - LEAN work will begin shortly to go through the day-to-day activities in lab and create standard work so that lab manager work along with that of the other CLS will be standardized. This should make time off less of a concern for the lab manager knowing that the day-to-day work is standardized, meaning that he can expect that all the standard work be completed upon his return and there will not be a stack of work that was unattended in their absence.
- Staffing
  - Lab is still working to get two (2) more CLS traveling or perm – to ensure that we can have a functional working manager and an adequate work life balance for staff when they do decide to take Mayers as an employer.

### ***Radiology***

- Radiology was able to operate through a critical staffing shortage. For some time the radiology manager was the only person working 7 days a week. Travelers have been interviewed and hired. Staffing will return to a more normal pattern as they all come on board.
- PCC Interface Once radiology is staffed and has capacity once again to be engaged in project work – we will begin work on completing the PCC interface with rad as well. (We have asked about all of

this work being valid when we change EHR and it should still be good work – we will just have to connect to the new EHR whatever that is)

- School site agreement -There is a potential agreement with the rad tech school in Yuba City – while there will not be high volumes of studies or other things that they students could potentially complete, there will be ample opportunity for the students to gain exposure to Mayers and to the demands and necessities of working as a rad tech in these frontier hospitals. This could be a fantastic benefit for recruitment and retention of techs in the future.

### **Chief Operating Officer Report**

**Prepared by: Ryan Harris, COO**

#### ***Facilities, Engineering, Other Construction Projects***

- The Demo project is continuing to make steady progress. Over the next two weeks, RHCI will continue with rough framing, Stephens electrical will start rough electrical, Lamb Unlimited will continue work on the fire and domestic water lines as well as finish grade, Ray-Mach Mechanical will start working on the HVAC work as soon as back-ordered parts come in and will start domestic plumbing, FC Brickert will also start exterior stucco the week of the 23<sup>rd</sup>. The contractor is scheduling the new fire line tie-in on August 27<sup>th</sup>. Work was also completed on the water tank pump project and the Architect of Record and Inspector of Record are finalizing the paperwork to close out that project. This project is still on budget and schedule.
- With the completion of the water tank pump project and the installation of the hood, we have started compiling the paperwork to get the final certificate of occupancy of the new hospital wing.
- Work continues on the laundry facility project. The contractor is targeting a completion date of October 15<sup>th</sup> 2021. The project is still on schedule.
- The daycare plans have been submitted to the county for approval. Shasta County came back with comments on August 4<sup>th</sup> and updated drawings were resubmitted to them on August 9<sup>th</sup>. At this time we are waiting on county approval to get bids from contractors to do the work.
- Alex and the maintenance team will once again be moving staff to accommodate the reopening of the COVID unit in OPM. Although no one wants to reopen this unit as we see more patients in the community and less availability to transfer a patient to other hospitals the COVID unit may be necessary. By doing the moves now it will make an easier transition in the event we have COVID patients admitted to the unit rather than waiting until we have them.
- Legionella issues were brought up during the Acute Mock Survey. Current plans are Phase 1: separate the domestic and fire lines in the demolition project and chlorinate the system. This is in the current OSHPD demo project. We received approval on an ACD to reroute all of our domestic water lines into the new riser room. This will give us three zones in our facility. Each zone will have its injection point of entry. This will help us as we will only have to shut down a zone at a time to do work on or chlorinate the system. As approved by the board at the last strategic planning session, we will be

replacing our water heaters now instead of during phase 3 which will also help remediate any future legionella issues we have.

- Hospital renovation project phase III was approved by the board in the last strategic planning session and preliminary work has started on the project. I am currently working with two architectural firms to see who can take on the project. The project includes a new kitchen in Fall River, new public and staff dining, new HVAC and water heaters for the entire facility excluding the new hospital wing, a change of use of our current dietary space to materials management and SNF storage. Staff is currently determining which building methodology - whether it be design build, design-bid-build or a hybrid of the two.
- Louis and I are currently discussing adding to the operations team a construction project manager owner representative. This person would take over a considerable amount of work and would be the point person for all district construction projects. This would also allow us to take on more projects at one time which will help speed up timelines of future projects. A job description has been made and is currently being reviewed by Louis.
- The final inspection with OSHPD for our acute nurse call project is scheduled for 8/19. Upon completion of this inspection we can start using our new nurse call system.

## *IT*

### Helpdesk

- In the last 30 days, we have seen a 10% increase in received tickets and a 4% increase in resolved tickets. This month we received more tickets than we were able to resolve. Our backlog increased by 55% to 70%.
- Average Response Time has decreased by 25% putting us at 3H28M, and Average Resolution Time has decreased by 33% putting us at 5H20M.
- We received a survey response on 52 of our tickets. 92% of our responses were 5/5, and 8% 4/5. We received no 3/5, 2/5, or 1/5.

### Projects

- New Pyxis Med Stations going live 8/23
- PCC Lab Interface Expected to go live this month
- Starting work on MVHC Lab Interface on 8/30

### Security

- Looking into expanding camera coverage with a vendor out of Chico
- Access Control system continues to have issues, vendor is scheduling us for a repair

## Operations Report

- Received bid for Managed Security Services to satisfy a critical BancSec audit finding related to event logging
- Received contract for remediating a critical BancSec finding related to Citrix access
- We are currently reviewing the other non-critical findings and establishing remediation plans through the Security Committee

### ***Purchasing***

- Nothing new to report at this time.

### ***Food & Nutrition Services***

- Staffing continues to be an area of concern in Dietary. We have implemented an incentive program for those employees who can pick up an extra shift. We are also developing a cross training program between dietary and EVS. We are also working on putting together a career fair where we will advertise our new sign-on and retention bonus program for EVS and Dietary.
- I want to thank all of our staff that volunteered to pick up shifts in dietary to cover the significant scheduling gaps we have in the department. The dietary staff and management greatly appreciate the willingness to help a department in need.
- Discussions and plans are taking being formulated to prepare for a reopening of the cafeteria to MMHD Staff. Due to staffing levels this has been put on hold until staffing levels return to normal.

### ***Environmental Services & Laundry***

- Staffing in EVS has also become a concern, having multiple resignations in the last month. We are taking a similar approach to EVS staffing and F&NS staffing.
- Sherry and I will be meeting next week to discuss the reopening and staffing plan for the Laundry facility when it reopens in October.

### ***Rural Health Clinic***

Amanda Ponti our Clinic Manager will be giving a more detailed monthly report to the board. This will be Amanda Ponti's last report to the board and she has made the decision to advance her career in the Electronic Medical Records field with OCHIN. If you speak with Amanda please join me in thanking her for all of the hard work and dedication in getting our clinic opened and through multiple surveys. I will be interviewing new candidates for the position the week of 8/23 with the goal of having Amanda spend some time with the new manager before she leaves on 9/17/2021.

**Operations District-Wide**  
**Prepared by: Louis Ward, CEO**

**COVID – 19**

Covid is once again spreading through the Intermountain area. We have seen an increase in the positivity rate in the area, which is depicted in the graph below. What we learn from the graph is the percentage of tests that are positive over a 7-day period of time. The reason we look for a snapshot and how it is changing over a 7-day period is it will tell us if there is a trend occurring and considering the numbers below we can determine there is more community members testing and when the test is resulted, it is determined to be positive for COVID-19.

<b>Total COVID Tests Performed (7 day trailing)</b>	<b>8/8/21</b>	<b>8/9/21</b>	<b>8/10/21</b>	<b>8/11/21</b>	<b>8/12/21</b>	<b>8/13/21</b>	<b>8/14/21</b>
<i>PCR- BIOFIRE</i>	2	1	3	2	0	1	0
<i>LABCORP</i>	0	25	21	20	12	7	5
<i>RAPID</i>	1	5	3	5	8	5	1
<i>Total COVID Positives (BIOFIRE)</i>	0	1	1	0	0	0	0
<i>Total COVID Positives (LABCORP)</i>	0	0	0	2	0	0	1
<i>Total COVID Positives (RAPID)</i>	0	0	0	0	1	0	0
<i>Total COVID Positive Positivity Rate (7 day trailing)</i>	1.33%	1.32%	1.81%	2.29%	3.76%	4.03%	4.72%

I did speak with the CEO of Mercy this week and they too are experiencing an increase in their numbers in Redding. At the time of writing this report, Mercy Medical Center has 54 COVID-19 inpatients, which is a new high for the facility. This is concerning as Mercy and Shasta Regional are full with patients, both COVID related and non-COVID related which makes transferring patients to higher levels of care more difficult. In response to this, Mayers will be adding 4 additional beds that will be located in an isolation space and be dedicated to caring for COVID patients.

We are also experiencing issues with our workforce quarantined due to exposures and not being vaccinated. At the time of writing this report we have 180/250 employees vaccinated which translates to 72% of staff.

**State Health Orders**

A number of new State Public Health Officer Orders were published in the last two weeks, which we are reviewing, implementing, and planning for. They are listed below:

- AFL 20-22.9 Guidance for Limiting the Transmission of COVID-19 in Skilled Nursing Facilities (SNF) - This revision requires SNFs to develop and implement processes for verifying the vaccination status of all visitors, and for obtaining and tracking

documentation of SARS-CoV-2 diagnostic test of all visitors who are unvaccinated and incompletely vaccinated to have an indoor visit.

- AFL 21-27 Coronavirus Disease 2019 (COVID-19) Testing, Vaccination Verification and Personal Protective Equipment (PPE) for Health Care Personnel (HCP) at General Acute Care Hospitals (GACHs) - This AFL requires hospitals to develop and implement processes for verifying the vaccination status of all HCP and for obtaining and tracking documentation of results of SARS-CoV-2 diagnostic screening testing from HCP who are unvaccinated or incompletely vaccinated and includes additional PPE requirements. These requirements are effective August 9<sup>th</sup> and should begin as soon as reasonably possible, with full compliance no later than August 23, 2021.
- AFL 21-31 Visitor Limitation Guidance at General Acute Care Hospitals - This AFL revision requires hospitals to develop and implement processes for verifying the vaccination status of acute care visitors and for obtaining and tracking documentation of results of SARS-CoV-2 diagnostic testing from visitors who are unvaccinated or incompletely vaccinated.

A State Public Health Officer Order was also released requiring all Healthcare Personnel in the state of CA to be fully vaccinated with some limited medical or religious exemptions by September 30<sup>th</sup>. This information has been shared with all MMHD staff. We are awaiting an All Facilities Letter for more details.

We are also working to understand a new federal announcement and regulation that all Skilled Nursing Facilities (SNF's) who do not have 100% of their staff vaccinated will lose all of their Medicare and Medicaid funding. At this point, they have not put a date on when this order goes into effect.

### **340B Contract with Mountain Valley Health Centers**

After much discussion, I am happy to report we have negotiated a new 340B contract with Mountain Valley Health Centers. This contract will make the 340B program more equitable to both parties. More information will be provided in Board Finance.

Respectfully Submitted by,  
Louis Ward, MHA  
Chief Executive Officer