Pre-Symposium Cyber TTX

After-Action Report/Improvement Plan

October 2021

The After-Action Report/Improvement Plan (AAR/IP) aligns exercise objectives with preparedness doctrine to include the National Preparedness Goal and related frameworks and guidance. Exercise information required for preparedness reporting and trend analysis is included; users are encouraged to add additional sections as needed to support their own organizational needs.

EXERCISE OVERVIEW

Exercise Name	Pre-Symposium Cyber Tabletop Exercise
Exercise Dates	October 19 1200-1430 In-Person
Scope	This is a Tabletop exercise, planned for two hours with the local, state, and federal partners. Exercise play is limited to identified stakeholders who registered for the pre-symposium tabletop exercise.
Mission Area(s)	Preparedness, Response, and Recovery
HPP Capabilities	• Capability 1 – Foundation for Health Care and Medical Readiness • Capability 2 – Health Care and Medical Response Coordination • Capability 3 – Continuity of Health Care Service Delivery
Objectives	1. Examine current organizational cyber incident response policies, plans, and protocols, and identify potential shortcomings or gaps. 2. Assess the preparedness of staff to respond to and manage cybersecurity incidents based upon your plans, policies, and procedures. 3. Identify alternative methods of care that meet your regulatory requirements in the event of a widescale cyber security incident that impacts your organization.
Threat or Hazard	Cyber Attack
Scenario	During a recent training event participants received a flash drive with all the required documents, templates, presentations, videos, and other resources discussed during the day. Unknown to the staff the flash drives purchased were infected with malware. Once the participants returned to their home, facilities, and agencies, they plugged the flash drive into their computers to review and download the files, which then infected the computer systems at their respective location.
Sponsor	City Ambulance Service SouthEast Texas Regional Advisory Council (SETRAC)
Participating Organizations	See Appendix B
Point of Contact	Adam Lee Regional Training and Exercise Coordinator 1111 North Loop West Suite #160 Houston, TX. 77439 281-822-4445 John Wingate Regional Training and Exercise Coordinator 1111 North Loop West Suite #160 Houston, TX. 77439 281-822-4439

ANALYSIS OF HPP CAPABILITIES

Aligning exercise objectives and HPP capabilities provides a consistent taxonomy for evaluation that transcends individual exercises to support preparedness reporting and trend analysis. Table 1 includes the exercise objectives, aligned HPP capabilities, and performance ratings for each HPP capability as observed during the exercise and determined by the evaluation team.

Objective	HPP Capability	Performed without Challenges (P)	Performed with Some Challenges (S)	Performed with Major Challenges (M)	Unable to be Performed (U)
Examine current organizational cyber incident response policies, plans, and protocols, and identify potential shortcomings or gaps.	Capability 1 – Foundation for Health Care and Medical Readiness		S		
Assess the preparedness of staff to respond to and manage cybersecurity incidents based upon your plans, policies, and procedures.	Capability 2 – Health Care and Medical Response Coordination		S		
Identify alternative methods of care that meet your regulatory requirements in the event of a widescale cyber security incident that impacts your organization.	Capability 3 – Continuity of Health Care Service Delivery		S		

Table 1. Summary of HPP Capability Performance

Ratings Definitions:

Performed without Challenges (P): The targets and critical tasks associated with the HPP capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Performed with Some Challenges (S): The targets and critical tasks associated with the HPP capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to

additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.

Performed with Major Challenges (M): The targets and critical tasks associated with the HPP capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

Unable to be Performed (U): The targets and critical tasks associated with the HPP capability were not performed in a manner that achieved the objective(s).

The following sections provide an overview of the performance related to each exercise objective and associated HPP capability, highlighting strengths and areas for improvement.

Objective 1: Examine current organizational cyber incident response policies, plans, and protocols, and identify potential shortcomings or gaps.

The strengths and areas for improvement for each HPP capability aligned to this objective are described in this section.

Capability 1 – Foundation for Health Care and Medical Readiness Strengths

The Partial Capability level can be attributed to the following strengths:

Strength 1: Stay vigilant in cyber security procedures.

Strength 2: Processes identified today for internal and external communications for a cyber incident.

Strength 3: Discussing and using past incidents to be better prepared for cyber security incidents.

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Update policies and procedures

Analysis: Many policies have been identified to have been out of date and requires updating to address new procedures and information.

Area for Improvement 1: Cyber training across all disciplines in healthcare, including refresher and new hire orientation.

Analysis: Cyber training has become relaxed in some areas and overlooked in annual trainings.

Area for Improvement 1: Following up on agreements in place for mutual aid

Analysis: Many MOA & MOU's have not been revisited since their development and may be out of date or require updating with new contact information and procedures.

Objective 2: Assess the preparedness of staff to respond to and manage cybersecurity incidents based upon your plans, policies, and procedures.

The strengths and areas for improvement for each HPP capability aligned to this objective are described in this section.

Capability 2 – Health Care and Medical Response Coordination Strengths

The Partial Capability level can be attributed to the following strengths:

Strength 1: Understanding the Downtime Procedures

Strength 2: Re-identification and re-imaging of software on computers

Strength 3: Regional working relationships with the Health Care Coalition

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Communications with patients and residents' family members

Analysis: Identify back up methods to notify patients and residents family members of significant incidents that could potentially affect their loved ones.

Area for Improvement 1: Staffing availability and shortfalls

Analysis: The COVID era has proven to us that we may lack the appropriate staffing to handle additional staffing demands presented from a cyber-attack.

Area for Improvement 1: Orientation and training of staff on the Emergency Operations Plan

Analysis:

Objective 3: Identify alternative methods of care that meet your regulatory requirements in the event of a widescale cyber security incident that impacts your organization.

The strengths and areas for improvement for each HPP capability aligned to this objective are described in this section.

Capability 3 – Continuity of Health Care Service Delivery Strengths

The Partial Capability level can be attributed to the following strengths:

Strength 1: Documentation during downtime and data restoration

Strength 2: Communication to restore trust in the facility from the public

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: Staff engagement post incident

Analysis: Many staff members have not been made aware of the activation process

Appendix A: Improvement Plan

HPP Capability	Issue/Area for Improvement	Corrective Action	Capability Element	Primary Responsible Organization	Organization POC	Start Date	Completion Date
HPP Capability: Foundation for Health Care and Medical Readiness	Update policies and procedures	Provide education on gaps in cyber response plans	HPP Capability 1	SETRAC	Training and Exercise	10/19/2021	04/30/2022
HPP Capability: Foundation for Health Care and Medical Readiness	Cyber training across all disciplines in healthcare, including refresher and new hire orientation.	Provide virtual cyber training through RACEDU	HPP Capability 1	SETRAC	IT	10/19/2021	06/30/2022
HPP Capability: Foundation for Health Care and Medical Readiness	Following up on agreements in place for mutual aid	Work with vendors to identify abilities to provide solutions during Cyber Incidents	HPP Capability 1	Facility Specific	SETRAC Coordinators	10/19/2021	Ongoing

HPP Capability: Health Care and Medical Response Coordination	Communications with patients and residents' family members	Validate plans to communicate with patients, residents, and family members during a cyber incident	HPP Capability 2	Facility Specific	SETRAC Coordinators	10/19/2021	Ongoing
HPP Capability: Health Care and Medical Response Coordination	Staffing availability and shortfalls	Identify staffing needs during down time of a cyber incident.	HPP Capability 2	Facility Specific	SETRAC Coordinators	10/19/2021	Ongoing
HPP Capability: Health Care and Medical Response Coordination	Orientation and training of staff on the Emergency Operations Plan	Work with onboarding to include location, and copy of the Emergency Operations Plan	HPP Capability 2	Facility Specific	SETRAC Coordinators	10/19/2021	Ongoing
HPP Capability: Continuity of Health Care Service Delivery	Staff engagement post incident	Develop or validate a plan for staff engagement and/or morale checks post incident	HPP Capability 3	Facility Specific	SETRAC Coordinators	10/19/2021	Ongoing

This IP has been developed specifically for the Healthcare Preparedness Symposium as a result of Pre-Symposium Cyber TTX conducted on 10/19/2021.

APPENDIX B: EXERCISE PARTICIPANTS

Ashton Parke Care Center	Memorial Hermann - TMC
Arkansas Healthcare Coalition SE region	Memorial Hermann Children's
Arkansas Hospital Association	Memorial Hermann Greater Heights
Arkansas HPP HCC	Memorial Hermann Home Based Services
Ashley County Medical Center SE Region	Memorial Hermann Orthopedic and Spine
Bayou Pines Care Center	Memorial Hermann Southwest
Beaumont Nursing and Rehab	Memorial Hermann TMC
Ben Taub Hospital	Modesty Home Health
Brighton Senior Living Cypress	Mount Belvieu Fire Department
Buckner Retirement Services DBA Parkway Place	OakBend Medical Center - Jackson Street
Capital Area of Texas Regional Advisory Council	Regent Care Center
Cartwright Homehealth	Regent care center at Kingwood
City of Wharton	Rice Medical Center
Clarewood House	SETRAC
Creative Solutions In Healthcare	Southern New Mexico Healthcare Coalition
Dogwood Trails Manor	St. Joseph Medical Center
Focused Care at Baytown	St. Lukes Heath Livingston
Fort Bend County Public Health	Sweeny Community Hospital
Gulf Coast Regional Blood Center	Texana Center
Health Care Temporaries Inc	Texas Children's
Hospital	The Medical Center of Southeast Texas
Houston Methodist West Hospital	The Orchard
Jefferson regional	Vidor Health and Rehabilitation
Liberty Dayton Regional Medical Center	Villa Toscana at Cypress Woods
Lufkin State Supported Living Center	West Wynde
Memorial City Health and Rehabilitation Center	