Fresno MHEPAC IT and Communications Systems Failure Tabletop Exercise (TTX)

Situation Manual

December 13, 2021

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

EXERCISE OVERVIEW

Exercise Name	Fresno MHEPAC IT System and Communications Failure Tabletop Exercise (TTX)
Exercise Dates	December 13, 2021, 15:00 – 17:00
Scope	This is a discussion based exercise, planned for two hours via Zoom. Exercise play is limited to Fresno County Medical Health Emergency Preparedness Advisory Committee (MHEPAC) members/participants.
Mission Area(s)	Response and Recovery
Core Capabilities	• Infrastructure Systems • Health Care and Medical Response Coordination • Continuity of Health Care Service Delivery • Situational Assessment
Objectives	• Identify facility systems/functions that would be lost; • Identify critical, immediate actions needed to avoid loss of life and other negative impacts to patients' health; • Identify processes and procedures to restore lost systems and to implement emergency actions until systems are restored; • Identify restoration priority for lost systems/functions; • Assess ability to continue operations during system outage.
Threat or Hazard	Hospital/healthcare facility IT and communications systems failure.
Scenario	Your facility's IT system and communications systems experience a significant failure and are unable to be brought back online immediately. The cause is not immediately known. IT failure affects environmental systems (heating/cooling), safety (fire alarms), electronic medical records, and other functions monitored and operated by the IT system.
Sponsor	Fresno County Department of Public Health (FCDPH) PHEP and HPP Programs and the Central California Healthcare Coalition, Fresno County Subcommittee (i.e. MHEPAC).
Participating Organizations	Fresno County Department of Public Health and hospitals and healthcare facilities located within the County of Fresno. See Appendix B.

Point of Contact

Darrel Schmidt, PHEP/HPP Program Coordinator
County of Fresno Department of Public Health
559-600-3149
DSchmidt@fresnocountyca.gov

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
Identify facility systems/functions that would be lost.	Infrastructure Systems
Identify critical, immediate actions needed to avoid loss of life and other negative impacts to patients' health.	Health Care and Medical Response Coordination, Continuity of Health Care Service Delivery
Identify processes and procedures to restore lost systems and to implement emergency actions until systems are restored.	Health Care and Medical Response Coordination, Continuity of Health Care Service Delivery
Identify restoration priority for lost systems/functions.	Health Care and Medical Response Coordination, Continuity of Health Care Service Delivery
Assess ability to continue operations until systems are restored.	Situational Assessment

Table 1. Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers.** Each participating facility may provide its own observers, if desired. Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Evaluators.** Each participating facility may provide its own evaluators, if desired. Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following modules:

- Module 1: Scenario Background - Initial Incident Information
- Module 2: Updated Incident Information – Next Steps
- Module 3: Considerations and Wrap-Up

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussion with the group.

Exercise Guidelines

- This will be a facilitated discussion with the entire group, without splitting into breakout groups.
- Answers to questions should be based on current plans, processes, and procedures.
- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and recovery efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
- The exercise scenario is plausible, and events occur as they are presented.
- All players receive information at the same time.

Exercise Evaluation

Each facility is encouraged to evaluate their responses to the exercise scenario questions and utilize this opportunity to identify areas for improvement within their plans, processes, and procedures. County staff will also draft an overall exercise AAR for distribution to attendees.

MODULE 1: SCENARIO BACKGROUND – INITIAL INCIDENT INFORMATION

January 12, 2022: 2:45 PM

Without warning, on January 12, 2022 at 2:45 pm, your facility's IT and communications systems experience a significant failure. IT staff are immediately aware of the occurrence and quickly perform a reboot of the system per normal operating procedures, but this is unsuccessful in bringing the systems back online.

Not realizing it is a systemwide failure, staff throughout the facility attempt to contact the IT department, but are unable to because the phone system has also failed. Within a few minutes facility staff who have each other's cell phone numbers are able to contact each other and IT staff and learn that all systems are down.

After approximately 15 minutes following the failure, IT staff are still uncertain what caused the failure or how to fix it.

Key Issues

- Power is fully functioning, but all facility systems operated/controlled by your IT system have failed. These include (but are not limited to):
  - Electronic medical records and access to other records accessed via your server
  - Environmental control system
  - Fire detection and alarm system
  - Phone system
  - Overhead PA system

Questions

Based on the information provided, participate in the group discussion concerning the issues raised in Module 1. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

<u>Mitigation</u>

1. Does your facility's plans address the threat and impact of an information technology (IT) failure in the annual Hazard Vulnerability Analysis (HVA), including the identification of mitigation strategies and tactics, and an analysis of all critical and non-critical IT systems?

Preparedness

1. Does your facility have an Information Technology Failure Plan? Does your facility exercise the Information Technology Failure Plan annually and revise it as needed?
2. Does your facility include preparedness strategies to reduce the impact from an information technology failure in your emergency management program and annual goals.
3. Does your facility establish criteria and procedures to activate a Command Center during emergencies, including who has the authority to activate the plan?
4. Does your facility have a Communications Plan that includes:
    a. Procedures for notification of events to internal and external authorities as appropriate?
    b. A plan to distribute radios and auxiliary phones to appropriate staff and facility areas?
    c. A plan for rapid communication of situation status to local emergency management and area hospitals, sister facilities, or like facilities that you may need to contact for patient support?
5. Does your facility have:
    a. An information technology system malfunction alert and notification procedure?
    b. Trained personnel for information technology response and recovery operations?
    c. Backup or alternate contingencies in place for communications, network failure, or equipment failure?
    d. Data backup and data redundancy processes and polices for enterprise wide and departmental specific data systems, including testing to ensure backups are functional?
6. Does your facility comply with current standards on disaster and emergency management and business continuity as they apply to all third party vendors that support and supply cyber technology services, such as offsite backup and data recovery processes?

MODULE 2: UPDATED INCIDENT INFORMATION – NEXT STEPS

January 12, 2022: 3:30 PM

IT staff believe they have identified the source of the failure. Assuming they are correct, they are uncertain how quickly the various systems can be brought back online. They estimate the minimum time needed is likely to be at least four hours, but it could be much longer.

A few staff are sent throughout the facility to notify each area that the system will be down for an unknown, extended period of time.

Key Issues

- IT staff believe they know the source of the failure, but are not 100% certain.
- Best case scenario is it will be a minimum of four hours before systems are back online. This timeframe assumes IT staff have correctly diagnosed the full extent of the root cause of the failure and no unexpected issues arise as they work to correct the problem.
- It will not be known whether any critical data has been lost until systems are back online.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 2. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Immediate and Intermediate Response:

Considering it will be an unknown, extended period of time before all systems will be functional:

1. Does your facility have systems and procedures to determine what information technology and other systems are affected by the incident?
2. Does your facility have communication methods to:
    a. Issue organizational alerts regarding information technology system failures?
    b. Determine contact lists and communication methods to immediately notify nursing staff and senior medical staff regarding affected information technology systems that will have direct impact on healthcare delivery and potential to adversely affect patient safety?
    c. Provide emergency incident notification when affected systems will take a significant amount of time to return to full operational status an to alert the Incident Commander and disaster recovery personnel?

d. Notify patients regarding any delays in service and the overall situation?

e. Implement regular briefings (as needed) on information technology systems restoration status for personnel?

3. Does your facility have procedures for all administrators and healthcare delivery staff to use manual documentation systems or unaffected portable devices and later merge data with recovered systems?

MODULE 3: CONSIDERATIONS AND WRAP-UP

Potential Causes

1. What types of circumstances could occur which would cause your facility's IT and communications systems to fail?

How would your facility's response change if circumstances differed as follows:

1. IT staff determine that restoration of all systems will take additional time, but they have the ability to prioritize which systems should be brought back first. How does your facility prioritize its systems?
2. After three hours, IT staff determine that their original diagnosis of the problem was incorrect and the failure is the result of a cyberattack.
3. The event causing the IT and communications systems to fail also caused an extended power loss.

APPENDIX A: EXERCISE SCHEDULE

Note: Because this information is updated throughout the exercise planning process, appendices may be developed as stand-alone documents rather than part of the SitMan.

Time	Activity
December 13, 2021	
3:00 pm	Welcome, Opening Remarks, Ground Rules, and Exercise Objectives
3:10 pm	Module 1: Briefing, Discussion, Q&A
3:50 pm	Module 2: Briefing, Discussion, Q&A
4:30 pm	Module 3: Briefing, Caucus Discussion, and Brief-Back
4:50 pm	Hot Wash
5:00 pm	Closing Comments

APPENDIX B: ANTICIPATED EXERCISE PARTICIPATING FACILITIES

Participating Organizations
Fresno County Department of Public Health
Adventist Health
American Ambulance
Avance Home Health
Bethesda Group Homes
California Association of Health Facilities
California Veterans Home
Central Valley Indian Health
Community Medical Centers
Department of State Hospitals - Coalinga
Fresenius Medical Care North America
Fresno American Indian Health Project
Healthcare Centre of Fresno
Hinds Hospice
Hospicecc.com
HumanGood
Kaiser
Maxim Health
The Nephrology Group
Omni Family Health
San Joaquin Valley Rehabilitation Hospital
Table Mountain Rancheria
Veterans Administration
Welbe Health
Willow Creek Healthcare Center

APPENDIX C: ACRONYMS

Acronym	Term
FCDPH	Fresno County Department of Public Health
MHEPAC	Medical Health Emergency Preparedness Advisory Committee
SitMan	Situation Manual
TTX	Tabletop Exercise