Hospital Emergency Communications

Interoperability & Redundancy Planning

IROQUOIS Healthcare Association

Updated January 2020

Contents

I. Overview

When normal communications methods of landline phone, cell phone and internet service are disrupted, alternate forms of communication must be relied upon. It is critical to develop redundant communication strategies in advance of such events.

In addition to accreditation standards requiring communications interoperability and redundancy, two key federal policies make this a priority for hospitals:

- **HHS ASPR's Hospital Preparedness Program** (2017-2022 HPP Cooperative Agreement) Requires at least two redundant communication drills annually to test the effectiveness of hospital and healthcare coalition communication systems and platforms (e.g., bed/resource tracking systems, amateur and commercial radio, satellite phones, etc.);
- **CMS's Emergency Preparedness Rule** (§482.15 Condition of Participation for Hospitals)[1] Requires that hospitals have a communication plan which includes primary and alternate means of communication, and that the communications plan be reviewed and updated at least every two years. The hospital must conduct two exercises annually which include testing the communications plan.

Redundant communications systems and platforms can include:

- Land lines - Hard-wired for internal/external communications;
- Cell phones and text messaging;
- Fax machines;
- Internet based communications used for E-mail, Voice over Internet Protocol systems, and reporting systems such as NYSDOH Health Commerce System (HCS), Health Alert Network (HAN), and Health Emergency Response Data System (HERDS);
- Satellite communication systems;
- Ham radio systems;
- Internal Radios - Two-Way Radio (UHF/VHF/800mhz);
- External Radios - 400/800mhz radio connectivity with county OEM,
  Motorola Radio System,
  Hospital-to-Ambulance Radio Frequency,
  Medical Emergency Radio System;
- Mass notification systems such as NY-Alert ;
- Emergency weather radio (for awareness of conditions that may impact operations);
- Human runners (the low-tech communication system if all else fails);
- Internal facility systems such as Intranet messages, overhead announcement and paging systems, nurse call system, Hospital television network systems.

[1] The Omnibus Burden Reduction Final Rule which took effect November 29, 2019 includes changes to the 2016 CMS Emergency Preparedness Conditions of Participation Final Rule (2016 EP Rule). Changes include decreasing from annually to biennially requirements for reviewing and updating the communication plan. Text of the requirements for hospitals showing these changes is available here.

II. Communications Plan

A. Complying with the CMS Emergency Preparedness Rule

The CMS Emergency Preparedness Rule (§482.15) requires that hospitals develop and maintain an emergency preparedness communications plan that complies with Federal, state and local laws. This communication plan should be reviewed and updated at least every two years.

The Communication plan should include how the facility coordinates patient care within the facility, across health care providers, and with state and local public health departments, as well as with emergency management agencies and systems to protect patients.

The communications plan should include the following contact elements:

- Names and contact information for the following:
  - Staff;
  - Entities providing services under arrangement;
  - Patients' physicians;
  - Other hospitals and CAHs;
  - Volunteers.
- Contact information for Federal, State, tribal, regional, and local emergency preparedness staff and other sources of assistance.

Contact information should be readily available and accessible to leadership and staff. The hospital should have a process to ensure that the information is accurate and current.

Primary and Alternate Means of Communication

Hospital communication plans should include primary and alternate means for communicating with their staff as well as federal, state, tribal, regional, and local emergency management agencies. The communication plan should include when and how alternate communication methods are used, and who uses them.

Additionally, hospitals should ensure that their selected methods of communication are compatible with the communications systems of those they need to contact. Any geographic communication difficulties or gaps should be outlined within the facility's risk assessment and addressed within the communications plan.

CMS' Interpretive Guidelines note that in determining the communication systems that best meet facilities' needs, they would consider: pagers, cellular telephones, radio transceivers (that is, walkie-talkies), and various other radio devices such as the NOAA Weather Radio and Amateur Radio Operators' (HAM Radio) systems, as well as satellite telephone communications systems.

The Interpretive Guidelines note that the Radio Amateur Civil Emergency Services (RACES) is an integral part of emergency management operations, and encourages hospitals to seek information about emergency communications services offered through the National Communication System (NCS) including: Government Emergency Telecommunications Services (GETS, Wireless Priority Service (WPS), Telecommunications Service Priority (TSP) Program, and SHARES.

Patient and Hospital Information

Communications plans should also include procedures and methods for information sharing needs including:

- Patient information and medical documentation with other providers to maintain continuity of care;
- HIPPA-compliant means to release patient information to family members in the event of evacuation;
- General information about the condition and location of patients in the hospital's care;
- Providing information to the jurisdictional Incident Command Center on the hospital's occupancy, needs, and ability to provide assistance to others.

B. Hospital Incident Command System

To ensure the Hospital Incident Management Team (HIMT) members are able to exchange information with internal hospital departments and external response agencies, the Hospital Command Center (HCC) should be equipped with redundant communication capabilities. The HICS Guidebook (Ch. 5.6.2) outlines the following equipment and supplies:

- ✓ **Voice systems**
  Includes telephones (land, cellular, satellite) and radio (amateur, commercial, and public safety 2-way radios). Antennas, repeaters, etc., should be provided as needed.
- ✓ **Data systems**
  Includes computers with modems on analog/digital lines, computers on a local or wide area network, and computers with wireless cards. Multiple data ports should be provided so all computers have internal connectivity in addition to external information sharing sites.
- ✓ **Equipment for receiving public broadcasts**
  Include multiple televisions or a large screen capable of showing multiple channels simultaneously and AM/FM and weather radios.
- ✓ **Equipment for visual display of incident information**
  Include large projection screens, whiteboards, maps, charts, and chart pads on easels.
- ✓ **Miscellaneous office supplies**
  In addition to preprinted HICS forms and general supplies, a fax machine and multiple photocopiers are necessary equipment.

It is important to periodically verify that the HCC equipment is functioning properly and that needed supplies are available on site. Information technology/information systems personnel should also verify that the computer software is updated and functioning as expected along with the primary and back-up communication systems.

III. Redundant Communications

A. Satellite Phones

As part of Iroquois Healthcare Association's Emergency Preparedness Communications Project, IHA purchased fixed and handheld satellite phones and laptop computers for rural hospitals in 2003 and 2004. Remaining hospitals were provided satellite equipment by the former Regional Resource Centers (RRCs).

In addition to voice communication when landline and cell phones are down, the satellite connection provides internet service for accessing email, NYSDOH data reporting, and hosted network services.

Purchased Equipment

The satellite phone equipment provided by Iroquois through grant funds included:

- ✓ **Globalstar Fixed Satellite Phone System (GSP-2900)**
  Enables voice, data and internet communication from phones and computers in the facility. Connects up to five analog ahones. System includes Radio Access Unit (antenna), mounting bracket, junction box, power/telephone cable, power supply, battery back-up, power cord.
- ✓ **Additional Battery for Fixed Satellite Phone**
  Second battery (GSP-2900) provides additional back-up power for fixed phone operation.
- ✓ **Globalstar Handheld Satellite Phone (GSP-1600)-**
  Provides voice and data services, including internet and email, voicemail, incoming SMS, and position location. Includes lithium ion battery (GSP-1210) and wall charger.
- ✓ **Additional Lithium Ion Battery (GSP-1210) and Battery Charger**
  Second lithium ion battery for handheld phone and handheld phone battery charger.
- ✓ **GSP-1600 Data Cable & IBM Thinkpad Laptop**
  Provides data connection with the handheld satellite phone. The data cable connects the handheld phone to a computer's RS232 port, laptop or PDA.
- ✓ **Handheld Satellite Phone Hands-Free Car-Kit (GCK-1410)**
  Includes Antenna, Module, Cradle, Hands Free Microphone, Speaker, 5m antenna cable.

Batteries

Iroquois purchased fixed and handheld replacement batteries for hospitals in 2006. The lithium ion battery that powers the handheld satellite phone has an expected life capacity of 300 cycles or charges, or about 3 years.

The fixed phone is connected to a battery which will power the phone during a loss of power for approximately 3 ½ hours of talk time and 24-48 standby. The battery will recharge itself upon restoration of power and has an extended life. In 2006 Iroquois purchased an additional battery to double the amount of operation time available during a power outage. If you need to purchase another fixed back-up battery, you may do so through many of your communication vendors.

Globalstar User Instructions and Software Updates

Below are links to Globalstar satellite phone user manuals and instructions:

Connecting and Using Fixed Satellite Phones Via Building Satellite Antennae

- GSP-2900 Fixed Phone System Overview
- GSP-2900 Quick Start Guide
- GSP 2900 Installation Guide
- GSP-2900 Supplemental Install Guide
- GSP-2900 User Guide

Using the Handheld Satellite Phone

- GSP-1600 Handheld Satellite Phone Overview
- GSP-1600 Quick Start Guide
- GSP-1600 User Manual

Additional Features

- Voicemail
- Call Forwarding

Service Plans, Billing & Customer Service

Globalstar's service agreement is a "Monthly Prepaid Plan", a monthly agreement with prepayment prior to each month. You may cancel the service plan 30 days prior to the end of such service month. To do so, call (877) 452-5782 and provide facility name, address and the product's Electronic Serial Number (ESN).

- Service Agreement General Terms and Conditions

The Online Invoice Center provides online access to your Globalstar statements. To update or change the contact information on your account, please contact Customer Care.

If your facility does not maintain satellite service, you may retain it for possible future use or return equipment purchased by Iroquois. If you wish to return equipment, please contact Andrew Jewett.

B. Public Alert Weather Radio

In 2006, Iroquois purchase a weather alert radio for all IHA member hospitals, rural hospitals in other regions, and hospital associations. The Midland WR100 Public Alert Weather Radio receives weather and public safety messages, enabling timely preparation and response.

C. Amateur Radio

Most hospitals in NYS have an amateur (or "ham") radio (see Equipment section below). Amateur radios must be operated by a licensed amateur radio operator. The Amateur radio may be used to communicate with emergency responders outside the hospital and can serve as a proxy for the hospital telephone system, should that system become dysfunctional. The primary modes of communication include:

- Voice transmission for short messages - Basic mode; available via base or portable radios;
- Digital transmission for lengthy reports and files – Sophisticated mode requiring specialized equipment and training; available at Command Posts or other facilities
- Phone Patch – Voice communications to specially equipped radio stations outside of the affected area that can connect their transceivers to the telephone network enabling HAM operators to communicate with one another much like a PBX system.

Radio Amateur Civil Emergency Services (RACES)

During emergencies Radio Amateur Civil Emergency Services (RACES) operators provide amateur radio communication when activated by a county emergency manager. RACES, regulated by the FCC, provides a pool of emergency communications personnel that can be called upon for emergency message handling on Amateur Radio Service frequencies. These operations typically involve messages between critical locations such as hospitals, emergency services, emergency shelters, and any other locations where communication is needed.

In addition to RACES units, there are individuals in the community who are authorized to use the amateur bands and who possess mobile, base, or portable equipment. Many of these persons are enrolled in the Amateur Radio Emergency Services (ARES) sponsored by the American Radio Relay League (ARRL). RACES is often combined with non-government ARES.

Hospitals have been encouraged to have a Memorandum of Understanding with the ARES/RACES team. The ARES/RACES team provides the hospital with the operator to assist the facility with communications. The ARES/RACES operator operates the radio; the facility controls the communication messages. Hospitals have been provided with an amateur radio and fixed antenna fixed. If there is no available radio or antenna, the ARES/RACES operator may provide the temporary infrastructure.

Amateur radio emergency nets convene at regularly scheduled times on specific frequencies. The NYS Office of Interoperable and Emergency Communications (OIEC) maintains a list of scheduled Emergency Services Nets, RACES regional contacts, as well as New York State RACES Standard Operating Procedure.

Please contact your county emergency manager to discuss amateur radio operation at your hospital during an emergency. For more information and to find local amateur organizations visit:

- RACES vs. ARES FAQs
- RACES and ARES Organizations
- HICS Job Aids - Emergency Amateur Radio Operator

Amateur Radio Equipment

Amateur radio equipment was purchased by Iroquois Healthcare Association in 2005 with NYSDOH Bioterrorism Grant funding for 77 hospitals. The equipment was provided to 54 Iroquois member hospitals and to 23 rural hospitals in Northern Metropolitan, Rochester and Western NY regions. Equipment purchased* included:

- Base Radio (Yaesu FT2800M) - TX 144-148 MHz freq. range, FM mode, high output-60 watts

- Base Radio Power Source (Samplex SEC-1223)
- Bulkhead mount (IS-B50LU-C1)
- Antenna (Diamond X-50A) - 5.5 feet high
- Radio to antenna feed line – 200 feet

** A different configuration was purchased for the five St. Lawrence County hospitals:*
(1) Kenwood TM-D700A VHF/UHF dual meter/440 radio
(1) Base radio power source (Astron SS25 20amp switching power supply
(1) Bulkhead mount (IS-B50LU-C1)

D. Emergency Phone Calls and Priority Service

During and following an emergency or disaster, mass calling by the public often triggers congestion in landline and cellular networks—forcing hospitals, emergency responders and other key personnel to compete with the public for the same overloaded communications resources.

Iroquois has worked with hospitals to establish the ability of hospitals and staff to make landline and mobile phone calls under emergency conditions and to have service restored on a priority basis. These programs, administered by the Department of Homeland Security Office of Emergency Communications (OEC), include:

- Government Emergency Telecommunications Service (GETS) - emergency calling card service that can be used from any telephone to provide priority for emergency calls.
- Wireless Priority Service (WPS) - an add-on feature subscribed on a per-cell phone basis to provide priority for emergency calls made from cell phones.
- Telecommunications Service Priority (TSP) - ensures restoration of TSP identified services before non-TSP services and facilitates priority installation of new telecommunications services in a shorter than normal interval.

NYSDOH HPP 2008-09 Deliverables required hospitals to obtain GETS and WPS accounts which were used during Interoperable Communications Exercise in 2009.

Government Emergency Telecommunications Service (GETS)

During emergencies, the public landline telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of essential service organizations and emergency response personnel to complete calls.

GETS provides essential personnel priority access and prioritized processing through landline networks, greatly increasing the probability of call completion. GETS has historically provided more than a 95 percent call completion rate during emergency response incidents.

Users receive a calling card providing access numbers, a Personal Identification Number (PIN), and simple dialing instructions. No special phones are required. You may place GETS calls from a cell phone. However, GETS calls over cellular networks are most effective when used in conjunction with the WPS.

There is no cost to enroll in GETS; the only charge for GETS is usage. GETS calls are billed at a rate of 7 to 10 cents per minute.

- How GETS Works
- GETS FAQs
- Making a Combined WPS and GETS Call
- Tips for Programming Smartphones for GETS and WPS Calls
- Helpful Tips for GETS and WPS Users

Wireless Priority Service (WPS)

WPS is designed to provide priority cellular calling capabilities when communications networks are congested. WPS has historically provided more than a 93 percent call completion rate.

The WPS service is added on a per-cell phone basis; calls must be placed on a subscribed phone to initiate priority calling. Callers dial *272 from an enrolled cellular phone followed by the destination number to make a WPS call.

WPS subscribers are responsible for initial enrollment, monthly subscription, and per-call charges. These charges vary by cellular carrier.

- WPS Fact Sheet
- Making a WPS Call
- Making a Combined WPS and GETS Call
- Tips for Programming Smartphones for GETS and WPS Calls
- Helpful Tips for GETS and WPS Users

Requesting GETS and WPS

Most organizations have a single point of contact (POC) who is able to submit GETS and WPS requests online. However, large or geographically dispersed organizations may elect to establish multiple POCs.

If you already know your organization's POC, please contact that individual to request a GETS card and/or enroll in WPS. Otherwise, you will need to do one of the following:

- Find out if your organization has a POC
- Change the POC for your organization
- Establish a POC for your organization

Once submitted, the DHS Priority Telecommunications Service Center will contact you within five business days to review your request. Supporting documentation may be required. Once approved, you will receive website login information (by email) and a GETS card (by U.S. Mail) within 10 business days. Notification of any WPS activations will be sent to you via email once the carrier provides enrollment confirmation.

- GETS and WPS User Organization Responsibilities
- GETS Facility Telecommunications Management

Telecommunications Service Priority (TSP)

The TSP program provides government agencies; public health and safety organizations, and others a way to receive priority installation and repair of critical data and voice communications circuits. The

FCC requires that service vendors prioritize requests for new or repaired circuits for organizations enrolled in TSP.

- TSP Priority for Emergency Communications
- TSP FAQs
- TSP Fact Sheets and Documents
- Requesting TSP

See Appendix B for a Telecommunications Service Priority (TSP) plan template which may be used in developing a facility plan.

TSP Provisioning and Restoration

There are two primary uses for Telecommunications Service Priority (TSP): one for installing new service (TSP Provisioning) and one for restoring existing service (TSP Restoration).

- **TSP Provisioning** - When circumstances require installation of a new service faster than a service vendor's normal processes allow, an organization may request provisioning priority. This can be an immediate installation following an emergency or an installation by a specific date, also known as an essential provisioning.
- **TSP Restoration** - Restoration priority is for new or existing services and requires that service vendors restore them before non-TSP services. Restoration priority helps minimize service interruptions that may have an adverse effect on the health and safety functions. Organizations must request TSP restoration priority before a service outage.

TSP Costs

TSP is a fee-based program and organizations pay their telecommunications vendor for the services. TSP set-up and recurring costs vary depending on the type of service requested, telecommunications vendor, and geographic location. Below is a table of approximate ranges of most TSP costs and is intended for informational purposes only. The vendor providing the service can supply actual costs.

TSP Provisioning *(non-recurring)*	**TSP Restoration** *(set up fee)*	**TSP Restoration** *(recurring Cost)*	**Change to Restoration** (*Priority Level)*
$50.00 - $416.00	$14.00 - $358.00	Up to $9.35 monthly	$2.91 - $131.00

TSP Enrollment Process

The enrollment and request process for TSP Provisioning and TSP Restoration is different, and details for each process are provided below.

The first step in the enrollment process is to establish a point of contact (POC) for your organization. Many organizations already have established POCs who facilitate the enrollment process. To determine your POC and enroll in the priority services programs, please contact the DHS Priority Telecommunications Service Center at (866) 627-2255.

Requesting TSP Provisioning

When circumstances require installation of a new telecommunications service faster than a service vendor's normal processes allow, an organization may request provisioning priority. This can be an

immediate installation following an emergency or an installation by a specific date, also known as an essential provisioning. These simplified steps show the basic process for requesting provisioning priority:

1. Call the DHS Priority Telecommunications Service Center toll free at 866-627-2255 for instructions on how to submit your request.
2. The Cybersecurity and Infrastructure Security Agency (CISA) will provide a TSP Authorization Code for each service or circuit you need to install, which you will give to your service vendor.
3. The vendor will confirm receipt of TSP Authorization Code(s) with TSP Program Office.

Requesting TSP Restoration

Restoration priority can be given to existing telecommunications, and requires that service vendors restore TSP assigned services before non-TSP services. Restoration priority helps minimize service interruptions that may have a serious, adverse effect on the supported NS/EP functions. Organizations must request TSP restoration priority designations on their circuits before a service outage. To request restoration priority designations on your circuits:

1. Please contact the Priority Telecommunications Service Center toll free at 866-627-2255, or via email at support@priority-info.com to determine program eligibility.
2. Once you are eligible, you will provide information about the services or circuits that need restoration priority. The TSP Program Office has up to 30 days to assign TSP Authorization Codes.
3. CISA will send you a TSP Authorization Code for each service or circuit.
4. Provide the TSP Authorization Code to your service vendor.
5. The vendor confirms receipt of TSP Authorization Code(s) with the TSP Program Office.

TSP Authorization Codes are active for three years, at which point the service user will need to revalidate them. Service users must request TSP restoration priority before a service outage occurs.

E. NY-Alert Notification System

The NY-Alert Mass Notification system is available to all NYS agencies and municipalities for public safety messaging. Other organizations such as hospitals and schools, can also utilize NY-ALERT for alerting. Contact NY-Alert Support at supprt@nyalert.gov with any inquiries.

NY-Alert enables hospitals to send out critical emergency information concurrently through email, phone and text. When an alert is issued, a brief description of the incident will be included in the message as well as recommended actions to be taken.

IV. Requirements, Standards and References

Below are references relating to redundant communications from CMS' Emergency Preparedness Rule and the Hospital Incident Command System (HICS) Guidebook. Hospitals should also reference their respective accreditation standards.

A. CMS Emergency Preparedness Condition of Participation for Hospitals

The hospital must comply with all applicable Federal, State, and local emergency preparedness requirements. The hospital must develop and maintain a comprehensive emergency preparedness program that meets the requirements of this section, utilizing an all-hazards approach. The emergency preparedness program must include, but not be limited to, the following elements:

§482.15(b) Development of EP Policies and Procedures

(b) Policies and procedures. The hospital must develop and implement emergency preparedness policies and procedures, based on the emergency plan set forth in paragraph (a) of this section, risk assessment at paragraph (a)(1) of this section, and the communication plan at paragraph (c) of this section. The policies and procedures must be reviewed and updated at least every two years. At a minimum, the policies and procedures must address the following:

(3) Safe evacuation from the hospital, which includes consideration of care and treatment needs of evacuees; staff responsibilities; transportation; identification of evacuation location(s); and primary and alternate means of communication with external sources of assistance.

(c) Communication plan. The hospital must develop and maintain an emergency preparedness communication plan that complies with Federal, State, and local laws and must be reviewed and updated at least every two years. The communication plan must include all of the following:

(1) Names and contact information for the following:
- (i) Staff.
- (ii) Entities providing services under arrangement.
- (iii) Patients' physicians.
- (iv) Other hospitals and CAHs
- (v) Volunteers.

(2) Contact information for the following:
- (i) Federal, State, tribal, regional, and local emergency preparedness staff.
- (ii) Other sources of assistance.

(3) Primary and alternate means for communicating with the following:
- (i) Hospital's staff.
- (ii) Federal, State, tribal, regional, and local emergency management agencies.

Interpretive Guidance:

Facilities are required to have primary and alternate means of communicating with staff, Federal, State, tribal, regional, and local emergency management agencies. Facilities have the discretion to utilize alternate communication systems that best meets their needs. However, it is expected that facilities would consider pagers, cellular telephones, radio transceivers (that is, walkie-talkies), and various other radio devices such as the NOAA Weather Radio and Amateur Radio Operators' (HAM Radio) systems, as well as satellite telephone communications systems. We recognize that some facilities, especially in remote areas, may have difficulty using some communication systems, such as

cellular phones, even in non-emergency situations, which should be outlined within their risk assessment and addressed within the communications plan. It is expected these facilities would address such challenges when establishing and maintaining a well-designed communication system that will function during an emergency.

The communication plan should include procedures regarding when and how alternate communication methods are used, and who uses them. In addition the facility should ensure that its selected alternative means of communication is compatible with communication systems of other facilities, agencies and state and local officials it plans to communicate with during emergencies. For example, if State X local emergency officials use the SHAred RESources (SHARES) High Frequency (HF) Radio program and facility Y is trying to communicate with RACES, it may be prudent to consider if these two alternate communication systems can communicate on the same frequencies.

Facilities may seek information about the National Communication System (NCS), which offers a wide range of National Security and Emergency Preparedness communications services, the Government Emergency Telecommunications Services (GETS), the Telecommunications Service Priority (TSP) Program, Wireless Priority Service (WPS), and SHARES. Other communication methods could include, but are not limited to, satellite phones, radio, and short wave radio. The Radio Amateur Civil Emergency Services (RACES) is an integral part of emergency management operations.

Survey Procedures

- Verify the communication plan includes primary and alternate means for communicating with facility staff, Federal, State, tribal, regional and local emergency management agencies by reviewing the communication plan.
- Ask to see the communications equipment or communication systems listed in the plan.

(c) Communication plan. *(continued)*

(4) A method for sharing information and medical documentation for patients under the hospital's care, as necessary, with other health care providers to maintain the continuity of care.

(5) A means, in the event of an evacuation, to release patient information as permitted under 45 CFR 164.510(b)(1)(ii).

(6) A means of providing information about the general condition and location of patients under the facility's care as permitted under 45 CFR 164.510(b)(4).

(7) A means of providing information about the hospital's occupancy, needs, and its ability to provide assistance, to the authority having jurisdiction, the Incident Command Center, or designee.

Interpretive Guidance:

Facilities in rural or remote areas with limited connectivity to communication methodologies such as the Internet, World Wide Web, or cellular capabilities need to ensure their communication plan addresses how they would communicate and comply with this requirement in the absence of these communication methodologies. For example, if a facility is located in a rural area, which has limited or no Internet and phone connectivity during an emergency, it must address what alternate means are available to alert local and State emergency officials. Optional communication methods facilities may consider include satellite phones, radios and short wave radios.

Facilities policies and procedures must outline primary and alternate means for communication with external sources for assistance. For instance, primarily methods may be considered via regular telephone services to contact transportation companies for evacuation or reporting evacuation needs to emergency officials; whereas alternate means account for loss of power or telephone services in the local area. In this event, alternate means may include satellite phones for contacting evacuation assistance.

(d) Training and testing. The hospital must develop and maintain an emergency preparedness training and testing program that is based on the emergency plan set forth in paragraph (a) of this section, risk assessment at paragraph (a)(1) of this section, policies and procedures at paragraph (b) of this section, and the communication plan at paragraph (c) of this section. The training and testing program must be reviewed and updated at least every 2 years.

(1) Training program. The hospital must do all of the following:

(i) Initial training in emergency preparedness policies and procedures to all new and existing staff, individuals providing services under arrangement, and volunteers, consistent with their expected role.

(ii) Provide emergency preparedness training at least every 2 years annually.

(iii) Maintain documentation of the training.

(iv) Demonstrate staff knowledge of emergency procedures.

(v) If the emergency preparedness policies and procedures are significantly updated, the hospital must conduct training on the updated policies and procedures.

(2) Testing. The hospital must conduct exercises to test the emergency plan at least twice per year. The hospital must do all of the following:

(i) Participate in an annual full-scale exercise that is community-based; or

(A) when a community -based exercise is not accessible, conduct an annual individual, facility-based functional exercise; or.

(B) if the hospital experiences an actual natural or man-made emergency that requires activation of the emergency plan, the hospital is exempt from engaging in its next required full-scale community-based exercise or individual, facility-based functional exercise following the onset of the emergency event.

(ii) Conduct an additional annual exercise that may include, but is not limited to the following:

(A) A second full-scale exercise that is community-based or an individual, facility-based functional exercise; or

(B) A mock disaster drill; or

(C) A tabletop exercise or workshop that is led by a facilitator and includes a group discussion, using a narrated, clinically-relevant emergency scenario, and a set of problem statements, directed messages, or prepared questions designed to challenge an emergency plan.

(iii) Analyze the hospital's response to and maintain documentation of all drills, tabletop exercises, and emergency events, and revise the hospital's emergency plan, as needed.

.

5.6 Establishing the Hospital Command Center (HCC)

5.6.2 Equipment and Supplies

To ensure the Hospital Incident Management Team (HIMT) members are able to exchange information with internal hospital departments and external response agencies, the Hospital Command Center (HCC) should be equipped with redundant communication capabilities.

- Voice systems include telephones (land, cellular, satellite) and radio (amateur, commercial, and public safety 2-way radios). Antennas, repeaters, etc., should be provided as needed.
- Data systems include computers with modems on analog/digital lines, computers on a local or wide area network, and computers with wireless cards. Multiple data ports should be provided so all computers have internal connectivity in addition to external information sharing sites.
- Equipment for receiving public broadcasts is necessary, including multiple televisions or a large screen capable of showing multiple channels simultaneously and AM/FM and weather radios.
- Equipment for visual display of incident information is also critical and includes large projection screens, whiteboards, maps, charts, and chart pads on easels.
- Miscellaneous office supplies in addition to preprinted HICS forms and general supplies, a fax machine and multiple photocopiers are necessary equipment.

It is important to periodically verify that the HCC equipment is functioning properly and that needed supplies are available on site. Information technology/information systems personnel should also verify that the computer software is updated and functioning as expected along with the primary and back-up communication systems.

Also see: 5.8 Communications and Coordination

V. Appendix

A. Determining Telecommunications Service Priority Requirements

Background

Costs associated with TSP make it too expensive to apply to every line. Still, state and local jurisdictions using telephone systems as a significant part of their emergency management functions should evaluate their need to participate in TSP. This evaluation will reveal whether sufficient backup systems and other counter-measures exist to ensure continued management of emergency operations. It also will show which specific circuits need to be under TSP.

Scope and Approach

This document provides guidance in evaluating whether telephone systems supporting emergency management should be part of the TSP system. The guidance uses a three-step process. First, check the system's individual components, looking at each in depth and not making any assumptions. Next, assess potential threats to the system and probable consequences. Finally, identify measures to minimize the threat or mitigate the consequences. (Many of these measures will not involve TSP. Indeed, their use may eliminate the need for TSP.)

Step 1 - Evaluation

The communications manager needs a thorough understanding of the telephone system. This includes identifying all elements of the system and understanding their interrelationships. Elements include all entities linked through the system. Examples include police, fire, and medical resources, as well as the Emergency Operations Center and the jurisdiction's political leaders. Having identified the elements, the manager must look at the network linking them together. Of course, the manager must have a conceptual understanding of the network's function. However, the analysis needs to be in depth, identifying each physical component. (Components include circuitry, local offices, repeaters, switches, cross-connections, microwave dishes, power sources, and any other hardware or software involved in the system.)

In completing the analysis, the manager needs to work with the service provider(s) or vendor(s), who can provide information on network components and facilities. However, the vendor may consider some information proprietary. If so, the vendor may be unwilling to provide complete responses to some questions.

To conduct a thorough evaluation of the system, managers need to ask specific questions.

1. How many vendors provide service and for which equipment? Look at both the network and at customer owned equipment. Managers also should investigate reselling of long distance service and other sub-contracts.
2. What are the common points of failure? Which facilities, equipment, or systems will affect other portions of the system if they fail?
3. Which local offices serve each segment of the network? If all segments come from the same office, this may be a single point of failure.
4. What facilities or equipment link different elements?

5. What types of facilities or equipment represent each segment of the system? (Example: copper wire or fiber cable, overhead or buried cable, microwave or landline, etc.)
6. How many possible points of failure exist with each component of the system?
7. Which components of the system have the highest point of failure?
8. What network management tools monitor the components of the network and identify problems?

In addition to assessing the network, the manager needs to assess contractual agreements with the vendors. This assessment must include a review of service agreements to determine existing measures to combat potential failures in any network element. Typical questions include the following.

1. What other emergency service systems exist in the area and how do they rank compared with the emergency communications system? What other services will compete for restoration during a widespread outage?
2. What restoration arrangements exist in the contract? How does the contract specify response?
3. Is there a strong working relationship among the service provider(s) and the network manager? If more than one provider, is there a strong working relationship among the service providers?

Step 2 - Assess Potential Threats

This step's purpose is to assess the vulnerability of the network. System managers should determine potential threats to the system as a whole, as well as to the individual components. This analysis should be exhaustive, identifying all possible threats to the system, regardless of the severity or the cause. Then rank the threats from the most likely to the least likely to occur.

Use the following questions to evaluate potential threats to the system. The aim is to set priorities by focusing on risk, which includes both probability and consequences.

1. What potential natural disasters threaten your system? (Be specific and include a range from minor to severe threats.)
2. What technological hazards pose a threat to your system?
3. What potential network failures threaten the functionality of the system?
4. Which components of the system would each potential threat affect?
5. Which components of the system are most vulnerable to the potential threats?
6. What are the effects on the system's functionality when a particular component is inoperable?

Step 3 - Identify counter measures to mitigate threats

Step 3 addresses the methods employed to counter the potential threats to the system or mitigate their effects. This step will assist system administrators in rating the survivability of each component identified in the first step. Evaluate the system's backup equipment, plans and procedures in cooperation with the service providers. Methods for mitigating the effects of the potential threats should be addressed for each component.

Consider the following questions when identifying counter measures.

1. What contractual restoration procedures are in effect for each component of the system? (Review service agreements for customer-owned equipment, as well as subcontractors to the principal vendor. Consider again the response time elements of these service contracts.)
2. What alternative services are available to combat potential threats to each segment of the system? (Samples include alternate routing, dual homing, custom calling features, foreign exchange, etc.)
3. Are radio, microwave, or cellular systems employed as backups to the system?
4. Which locations have working, regularly load-tested backup power sources?
5. Is standby equipment available at each site within the system? (This is a key question. If a component or circuit isn't important enough to provide backup, it probably doesn't warrant TSP.)

Application of TSP based on results

The methodology helps assess whether sufficient methods are available to alleviate the effects of potential threats on emergency service communications systems. It provides system managers with a basis for identifying vulnerable areas in the system. Following this methodology will help determine whether participation in the TSP System is warranted. In general, TSP is not appropriate for all segments of the network. The Federal Communications Commission never intended TSP to provide total coverage. However, addressing each component of the system separately might identify areas where a TSP assignment would be prudent.

Based on the results of the evaluations in the methodology, TSP might be applicable to the following situations:

- Facilities within the system use more than one service vendor.
- Network components have single points of failure.
- Vendor relations are unsteady or questionable, or past vendor service has been poor.
- Segments of the service where diversification alternatives are limited or insufficient.

System administrators should use the results of the methodology to determine areas where TSP would be helpful. Further, good vendor relationships combined with a high visibility system might mean timely response to failures without a TSP assignment. Regardless of the mitigation method one ultimately chooses, this methodology will assist in determining the survivability of your system.

B. Telecommunications Service Priority Plan Template

[HOSPITAL NAME]

TELECOMMUNICATIONS SERVICE PRIORITY (TSP) PLAN

PURPOSE

The purpose of this plan is to describe [Hospital Name's] policy for the Telecommunications Service Priority (TSP) system. TSP is a Federal Communications Commission (FCC) program that directs telecommunications service providers to give preferential assistance to users enrolled in the program when they need lines restored following disruption of service. The activation of this plan will have telecommunication lines restored on a priority basis by the carrier(s) following disruption of service regardless of cause as required by the Federal Communications Commission (FCC). Participation in this program will enable healthcare system communications with first responders (police, fire, ambulance) as well as with state and local health departments during critical times.

OBJECTIVES

The objectives of this plan are to:

- Identify staff needed to complete TSP enrollment
- Identify circuits or lines TSP enrollment
- Describe process to request restoration priorities from carrier
- Obtain restoration codes from TSPPO
- Document codes & TSP enrollment with the carrier(s)
- Develop a TSP policy for use during a service outage

ESTABLISHING & MAINTAINING TSP CIRCUITS & LINES

- Staff overseeing the TSP program include:
  - Director of Information Services (IS) – Oversees enrollment and maintenance of the program
  - IT Manager – collaborates with the IS & TSP to maintain connectivity
  - Materials Management & Accounts Payable – Attend to placing the order and paying bills
  - Emergency Preparedness Coordinator assures completion & ongoing TSP coverage
  - Environment of Care/Emergency Management Committee oversees overall program
- Circuits & lines included in TSP restoration priority include those needed for communication with emergency responders, state & local health departments, telemedicine such as medical imaging, data transfer, and for transferring patient information. These circuit and lines are identified in Attachment A
- Restoration priority requests from carrier(s):
  - Contact our carrier & notify them of our intent to implement TSP restoration
  - Ask about additional charges that may apply
  - Ask how the TSP codes must be conveyed to them for enrollment i.e. spreadsheet via email or change service order
  - Ask the carrier the appropriate 24/7 contact information in the event restoration is needed during an outage

- Restoration priority can be given to existing telecommunications, and requires that service vendors restore TSP assigned services before non-TSP services. Restoration priority helps minimize service interruptions that may have a serious, adverse effect on the supported NS/EP functions. Organizations must request TSP restoration priority designations on their circuits before a service outage. To request restoration priority designations on your circuits:
  1. Please contact the Priority Telecommunications Service Center toll free at 866-627-2255, or via email at support@priority-info.com to determine program eligibility.
  2. Once you are eligible, you will provide information about the services or circuits that need restoration priority. The TSP Program Office has up to 30 days to assign TSP Authorization Codes.
  3. CISA will send you a TSP Authorization Code for each service or circuit.
  4. Provide the TSP Authorization Code to your service vendor.
  5. The vendor confirms receipt of the TSP Authorization Code(s) with the TSP Program Office.
  6. TSP Authorization Codes are active for three years, at which point the service user will need to revalidate them. Service users must request TSP restoration priority **before** a service outage occurs.
- 24/7 Contact for carriers listed above serving TSP Enrolled lines are listed in Attachment A.
- Process for requesting priority restoration during a service outage: The request for restoration or adding emergency lines can be made by AOD, [Incident Commander, IS Director or lead IS personnel, Nursing Supervisor or other individual who has the authority or training].
- Maintenance of this policy is the responsibility of the hospital's [IT Manager/ IS Director and Materials Management Director]. Periodic [annual, quarterly] updates, review and coordination will be the responsibility of the hospital's [IT Manager/ IS Director and Materials Management Director and reported through the Emergency Management Committee].
  This policy was developed and reviewed by the [Emergency Management Committee, IT Manager/ IS Director and Materials Management Director, and the Emergency Management Coordinator].

REFERENCES

This plan contains information from various sources including the National Communications System (NCS) website at https://www.dhs.gov/telecommunications-service-priority-tsp**.**

DHS CONTACT INFORMATION

DHS Priority Telecommunications Service Center toll free at 866-627-2255 or via email at support@priority-info.com.

APPENDIX A

Line Number	Carrier	TSP Code	24/7 Carrier Contact
1234	Verizon	TSP0A2M6C-03	800-555-1212

APPENDIX B – [Attach carrier confirmation of enrollment].