Health care facilities may experience interruptions to their information technology (IT), software applications, and telecommunications services for various reasons (e.g., hardware failures, network congestion, secondary effects of power outages, and damage to lines and cables, telephone poles, cellular towers, networks, switching centers, and communications satellites). Interruptions may be due to natural disasters and other unintentional incidents or human-caused acts such as cyberattacks and critical infrastructure sabotage. A multidisciplinary team including planners, engineers, IT administrators, clinical leaders, risk management, compliance, public relations, and others should be aware of services that could be affected by telecommunications and IT outages and develop redundant processes to maintain safe operations and allow for the continuity of care. Health care facility planners should conduct and/or participate in exercises with telecommunications providers, IT vendors, and key response partners in their community to verify and test system resiliency.

Utility Failure Tip Sheet
TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Health care facility emergency planners can incorporate the following considerations when determining their specific telecommunications and IT system needs:

- Identify critical telecommunications and IT services, their interdependencies with each other, and their dependence on electrical and other utility services.
- Use multiple internet and cellular providers when possible to enable a seamless transition to an alternate provider if service is interrupted or lost.
- Modernize legacy systems (i.e., outdated software and hardware) and, where practical, move towards virtual data centers and cloud-based services.
- Enroll in Department of Homeland Security Priority Telecommunications Services (Government Emergency Telecommunications Service [GETS], Wireless Priority Service [WPS], Telecommunications Service Priority [TSP]).
- Identify and deploy alternate technologies to support voice communication, text, data management, and information sharing, including exploring the use of a satellite internet constellation.
- Establish process to rapidly assess the effects of a telecommunications or IT failure and determine whether to activate incident command.
- Follow processes outlined in business continuity plan.
- Determine alternate methods of communicating laboratory results, executing pharmacy orders, transmitting radiology results, and accomplishing other processes involving clinical information while maintaining Health Insurance Portability and Accountability Act (HIPAA) and personally identifiable information (PII) compliance in the event of a failure.
- Increase staffing and/or develop a "pool" to reassign staff to complete tasks that can no longer be automated to help ensure patient and staff safety.
- Predetermine triggers that may warrant diversion, transfer of patients, or evacuation if safe operations cannot be maintained.
- Identify technology dependent services (e.g., telehealth, translation) that may need to be reduced or provided via alternate means and how to communicate this to patients and their loved ones.
- Post updates for staff and the community on websites and social media (or traditional media if internet is not functional). Educate staff on where to look for updates.
- Predevelop internal and external messaging focusing on multiple modes of communication.
- Work with vendors and emergency management agencies to ensure facility is considered priority for restoration.
- Ensure emergency contracts are in place with vendors to repair or replace damaged hardware and include requirements such as priority status, expected response time, and cost. Review contracts at least annually with the service provider to ensure mutual understanding and ability of the provider to execute.

ASPR
Administration for Strategic Preparedness and Response
TRACIE
Healthcare Emergency Preparedness Information Gateway

- Maintain printed directory of 24/7 contact information and notify critical partners (e.g., emergency medical services, health care coalition, emergency management agency, nearby health care facilities, public safety dispatch centers, law enforcement) of outage status and potential impacts on operations. Establish alternate information sharing mechanisms as needed.
- Follow reporting and other requirements associated with interruption, loss, or restoration of telecommunications and IT services.

N TELECOMMUNICATIONS

C

- Identify alternatives (depending on the outage type) to landline, wireless, and Voice over Internet Protocol (VoIP) phones. These may include analog phone lines, cellular phones, satellite phones, amateur radio, portable radios, pagers, public address systems, and runners.
- Ensure electricity dependent telecommunications are connected to backup power source.
- Maintain clinical unit and staff contact lists with alternate contact methods.
- Plan how and when alternate communications will be distributed and consider the additional staffing needed to disseminate timely and accurate information.
- Maintain a validated and printed directory of analog telephone numbers used in the facility.
- Maintain supplies to support alternate communications (e.g., mobile phone chargers, radios, batteries).
- Consider using an independent mass notification system to communicate with staff and other stakeholders.
- Incorporate communications failure into training and exercises to test staff, equipment, and procedure readiness.
- Forward VoIP calls automatically to designated mobile devices during outages.
- Post status updates for staff on facility intranet. If not available, use message boards and other methods.
- Record updates on voicemail system.
- Ensure TSP and WPS are activated, if enrolled.
- Explore with emergency management partners and vendors the availability of cell on wheels or other portable cellular sites.
- Reroute calls to an alternate location (e.g., call center, another facility in the health system) if available.
- Contact emergency management agency and non-governmental organizations to determine if they can provide HIPAA-compliant phone banks or other communication support.

KEY — N Need — C Considerations

N INFORMATION TECHNOLOGY

C

- Publish and maintain an IT Disaster Recovery (DR) plan, harmonize it with the Business Continuity Plans (BCP) used by the facility, and test it at least twice per year. Comprehensive DR and BCPs should include:
  - » Acknowledgement and descriptions of the facility's major risks, vulnerabilities, and dependencies.
  - » Maps of the entire IT infrastructure to identify interdependencies and plan the order of restoration of systems.
  - » Established clinical and non-clinical downtime workflows, triggers, and a clear communication plan to alert facility staff of their activation.
  - » A regularly updated and thorough list of key hardware, software, biomedical devices, and data.
  - » List and location of networked devices that can function in a non-networked mode.
  - » Segregation of life safety equipment and security communication platforms onto isolated networks with established redundancies in alerting, alarms, and notifications.
  - » Use of downtime computers that contain copies of key medical record data and can be connected to backup power.
  - » Adherence to industry and federal guidance for system segmentation/partitioning where networks, functionality, and IT components are separated to control access and strengthen network security.
  - » Maintenance of downtime supplies, such as forms, copiers/printers, toner, paper, pens/pencils, USB drives, and cellular data "hot spots" and ensure staff know where they are located and when and how to use them.
  - » Clearly defined reporting procedures for cybersecurity incidents that include requirements for immediate escalation and protocols for rapid system shutdowns/partitioning to prevent further damage.
  - » Tested procedures that ensure patient registration and insurance coverage information is correctly recorded. Consider using prepopulated patient IDs for mass casualty incidents and IT system failures to help decrease delays with test orders. Determine alternate ways of managing copays.
  - » Tested procedures on how to track time and pay staff if payroll systems are affected.
  - » Established process for back charting or scanning downtime charts during recovery.

N TELECOMMUNICATIONS CONTINUED

C

- Use virtual servers running on redundant host hardware in multiple, physically distinct locations with a back-up power source.
- Include DR plans with specified recovery time objectives (RTO) and recovery point objectives (RPO) in contracts with cloud service providers (e.g., Microsoft Azure, Amazon Web Services, Google) for cloud and hybrid cloud datacenter configurations to provide continued service in the event of hardware failures, software failures, or loss of connectivity at or within the host company's facilities.
- Ensure physical hardware required to run critical software applications is redundant and housed in physically distinct locations with a back-up power source.
- Address needs of personnel working remotely.
- Notify third party payors of issues with billing systems to establish workarounds and avoid penalties.
- Plan to increase staffing to assist with recovery documentation.
- Identify what patient data is needed for transporting patients to other facilities when electronic medical records cannot be accessed.
- Include information on downtime procedures in annual disaster training. Ensure staff are trained in their own department's procedures as well as have familiarity with the procedures of ancillary departments.

KEY N Need C Considerations

Related ASPR TRACIE Resources

- Utility Failures Topic Collection
- Communication Systems Topic Collection
- Healthcare System Cybersecurity Readiness and Response Considerations
- Identifying and Overcoming Communications Vulnerabilities: Nashville, TN
- Utility Failures in Health Care Toolkit

Other Resources

- Priority Telecommunications Services | CISA
- Resilient Power Best Practices for Critical Facilities and Sites with Guidelines, Analysis, Background Material, and References