IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

EMERGENCY COMMUNICATIONS BEST PRACTICES FOR ESTABLISHING ALTERNATE CARE SITES

OVERVIEW

This document provides unique considerations for state, local, tribal, and territorial (SLTT) entities establishing communications capabilities for Alternate Care Sites (ACS) during a health crisis or other disaster, such as crucial roles and coordination points, recommendations for ensuring the availability of critical communications services, and cybersecurity. The methods and means for establishing ACS communications may vary by state, county, locality, tribe, and territory; therefore, the information provided is not meant to be comprehensive.[1] Instead, this document intends to identify and share communications resources and best practices to fill an observed need for consolidated guidance when establishing ACS.

ACS TYPES, IDENTIFICATION, AND SELECTION

Although multiple names are used to describe these sites[2], this document refers to them, generally, as ACS for consistency and defines them as facilities temporarily converted, constructed, or repurposed for healthcare use during a public health emergency to reduce the burden on hospitals and established medical facilities.[3] **Those coordinating communications for the ACS should be included in initial and ongoing discussions among SLTT management, public health, and government entities** who use site selection and prospective patient care levels to inform an assessment of organic communications capabilities and supplemental communications requirements. In most cases, **leveraging buildings or even vessels** (e.g., hotels, armories, civic or convention centers, stadiums, schools, community centers, ships) **with pre-existing infrastructure simplifies coordinating logistical requirements.**

Federal ACS Guidance

- Centers for Disease Control and Prevention Considerations for ACS provides guidelines for establishing ACS
- Federal Healthcare Resilience Task Force ACS Toolkit was adapted from the Department of Health and Human Services (HHS) Federal Medical Station Concept of Operations (CONOPs)
- HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE) hosts ACS best practices
- USACE ACS resources provide general guidance, including site assessment templates
- Federal Emergency Management Agency (FEMA) Emergency Protective Measures Fact Sheet provides a list of emergency medical care activities eligible for funding

Site Types[4]

Type I (e.g., Federal Field Hospital): Patient surge capacity of ~1000+; rare instances reserved for large metropolitan areas or highly affected regions; typically managed by federal entities, such as the U.S. Army Corps of Engineers (USACE) or the National Guard:

- **Examples:** U.S. Navy Ship Comfort and Javits Convention Center; New York, NY
- **Communications Coordination: Tactical communications[5] tend to be self-sufficient** and managed by federal entities

Type II (e.g., Field Medical Station): Patient surge capacity of ~500–1000; instances reserved for mid/large

[1] In April 2020, information was collected from open-source data as well as the Cybersecurity and Infrastructure Security Agency's (CISA) emergency communications coordinators who work in the field with local organizations, counties, states, tribes, and regions.
[2] Other names: temporary healthcare facility, federal field hospital, portable hospital, field medical station, temporary hospital, remote hospital deployment
[3] U.S. Army Corps of Engineers. www.usace.army.mil/Coronavirus/Alternate-Care-Sites, last accessed August 6, 2020.
[4] Site type classification varies within plans and templates nationwide; the categories included in this document were created to reflect patterns in the way state and regional coordination was referencing them during the 2020 health crisis.
[5] Tactical communications refer to "communications between on-scene command and tactical personnel and cooperating agencies and organizations." Federal Emergency Management Agency (FEMA) (2017). *National Incident Management System*. Third Publication. Retrieved from: https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf.

urban/suburban areas or highly affected regions; often federally sponsored and supported, but executed through the state:

- **Example:** New Jersey Convention Center; Edison, NJ
- **Communications Coordination: State-assisted telecommunications coordination with potential support from federal entities** (e.g., survey, site selection, gap analysis); SLTT governments work with federal entities, such as the Federal Emergency Management Agency (FEMA), as required, to secure funding for their communications needs

Type III (e.g., Local ACS)[6]: Patient surge capacity of ~500 or less; often deployed in smaller urban areas and suburban or rural communities; may be initiated by SLTT governments:

- **Examples:** Connecticut Task Force, appointed by the Governor, site assessments for ACS performed throughout the state (March 2020); Multiple Sites, CT
- **Communications Coordination: SLTT governments may work in coordination with a federal entity** to assist in site identification **and often self-assess, deploy, and demobilize communications needs** without further need for supplemental provision or management

COORDINATING AND OPERATIONALIZING SUCCESSFUL ACS COMMUNICATIONS

Early coordination and a better understanding of the long-term mission help define appropriate communications requirements from the beginning. Communications coordinators increase their likelihood of success by 1) leveraging existing plans; 2) knowing key points of coordination (both government and industry); 3) performing on-site assessments to anticipate immediate and long-term communications requirements; 4) knowing how to prioritize ACS services; and 5) identifying infrastructure and cybersecurity requirements and who will address those needs. The following sections provide additional information on following these best practices throughout ACS deployment and demobilization/decontamination.

Plans, Tools, and Templates

Leveraging well-thought out guidance and templates can assist in the development of prescriptive ACS response plans. Whether faced with having to quickly establish an ACS without a pre-existing plan or building a plan during non-crisis times, the HHS ASPR TRACIE portal provides relevant resources and technical tools on:

- Site Selection Matrices
- SLTT Toolkits to Assist with Establishing ACS
- ACS Decision Frameworks
- ACS Lifecycle Concepts, Models, and Process Flowcharts
- ACS Sample Plans and Templates

Leveraging, Executing, and Revising Existing Plans

Ideally, local or county governments considering deploying ACS have already written, employed, and exercised a CONOPs, or other operational plan, in coordination with their local, county, and state health departments that includes ACS considerations for when hospitals are overwhelmed. Often referred to as an **ACS CONOPs Plan**, this document not only **considers unique characteristics of the area to properly identify and select a site location, provide adequate staffing and supply levels, and streamline operations**, but **reflects logistics and coordination communications and Information Technology (IT) requirements unique to a public health crisis.** Information within an ACS CONOPs plan may include, but is not limited to, potential event scenarios; surge response levels (including state or federal assistance or State Medical Response Team support); site types determined by scenario types; scope of patient care (level and type); site potentials and physical characteristics based on pre-event site assessments (e.g., location, size, layout, infrastructure and capabilities, security); population demographics and social vulnerabilities to the area; staffing recruitment and training needs; credentialing and patient-tracking processes; logistics operations and support (e.g., supply chain and equipment/support provision); site activation and support sequence; patient transportation needs; demobilization processes, and key points of contact.

Healthcare requirements during health crises are often unpredictable, potentially requiring those executing the plan to adapt operations as the event unfolds. **Lessons learned should be recorded at various execution stages to ensure data on successes and challenges are documented and incorporated back into the plan** following the event.

[6] There is a greater need to provide best practices and guidance to smaller ACS as the communities standing up these facilities often draw from limited resources, require additional coordination with federal entities and service providers to supplement coverage in ad hoc ways, and are less likely to have recently updated and exercised CONOPs or operational plans across the community.

Key Roles and Sources of Coordination

Even in the wake of a major public health crisis, response efforts start at the community level. In almost every case, deploying ACS requires coordination across various institutions, disciplines, levels of government, and industry starting at the local or county levels to identify need, sponsors, patient care, facility requirements, and potential sites. Ideally, a Unified Command, as defined in the Incident Command System (ICS)[7], will assist coordinating communications aspects of the public health crisis across jurisdictions, including ACS activation.

Roles of Communication Unit Leaders (COMLs) and Information Technology Service Unit Leaders (ITSL) for Coordinating ACS

COMLs and ITSLs bring value to ACS communications coordination and deployment and should be involved in coordinating ACS communications, when possible. A position within the ICS, COMLs develop plans for effective incident communications equipment and facilities use, manage communication equipment distribution, and coordinate installation and testing. A COML determines the appropriate communications requirements, including programming and deploying radios as well as mitigating interference. **In many cases of local or county communications coordination for ACS, COMLs can conduct site assessments to identify communications capabilities, define the communications requirements, determine gaps, and coordinate deployment and demobilization of support and assets.**

COML Areas of Expertise

To inform response and ACS deployment during a health crisis or other disaster, COMLs often have critical knowledge of:

- Local communications and systems
- Frequencies and spectrum
- Patching technologies
- Local topography
- System site locations
- SLTT communications plans
- Regional and local Tactical Interoperable Communications Plans, if available
- Communications and resource contacts
- ICS 300 level training

The ITSL has knowledge and expertise in IT, and is needed to provide information management, wired and wireless network requirements, cybersecurity, and application management in response to incidents, including Incident/Unified Command Post, Incident Communications Centers, Medical Control Operations Centers and various tactical operations centers, joint information center (JIC), staging areas, and field locations. **The ITSL is able to fulfill critical needs for sufficient access to broadband data, applications, and systems for ACS.**[8]

Other Key Coordination Points

Emergency communications personnel from the local or county Emergency Operations Center (EOC) should consider **maintaining regular contact with the following key personnel across all levels of government and between emergency management and healthcare entities** to properly coordinate site selection, conduct assessments, develop requirements, and assist the operationalization and demobilization stages of ACS deployment:

- State EOC
- Emergency Support Function (ESF)-2 Lead
- ESF-8 Lead
- Statewide Interoperability Coordinator (SWIC)
- FEMA Regional Administrators
- Department of Health and Human Services (HHS) Regional Administrators
- Emergency Medical Services (EMS) Administrators and Medical Directors
- Hospital Medical Directors and Administrators
- ACS Operations Manager(s)
- Communications Industry/Private Sector Leads
- Cybersecurity and Infrastructure Security Agency (CISA)'s Regional Directors

[7] In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, Unified Command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

[8] Depending on how the ACS is used, COMLs and ITSLs may coordinate with SLTT public safety entities—potentially including EMS, 911 Centers or Public Safety Answering Points (PSAPs), and Emergency Communications Centers (ECCs)—to integrate new ACS communications capabilities and requirements into existing response and hospital transport plans. Inclusive staffing of critical personnel ensures the ACS is effective when establishing necessary capabilities, such as EMS patient transport communications or dispatch needs.

Information Sharing Platforms during Health Crises

Coordinating entities should use shared and trusted platforms as much as possible to exchange crucial information during public health crises.[9] The following may be used to support critical information exchange during an event, ranging from cleared public information to information and coordination exchange relevant for incident and crisis management for ACS:

- Centers for Disease Control and Prevention (CDC)'s Health Alert Network
  Provides cleared, public health information alerts
- HHS Health Information Exchange
  Supports secure exchange of clinical information among different information systems to support patient-centered care
- Homeland Security Information Network
  Shares sensitive but unclassified information among the Department of Homeland Security's (DHS) federal, SLTT, and international partners

Meeting ACS Mission Requirements: Assessments, Gap Analyses, and Resource Deployment

Following site selection, communications coordinators will need to reference existing plans and coordinate closely with the ACS Operations Manager to determine communications requirements. Next, an assessment will need to be performed of the site's existing capabilities as well as a gap analysis to identify the need for and availability of auxiliary capabilities and services. The following list is not comprehensive, but it may assist with initial steps to generate ACS communications requirements; achieve operable, interoperable, reliable, resilient, and secure ACS voice, video, and data needs; and mitigate disruptions to or shifts in service and capabilities.

Meeting ACS Mission Requirements during Site Identification, Selection[10], and Deployment

Communications coordinators should be included when identifying sites, determining opportunities to leverage existing infrastructure, and identifying additional need to meet coverage, capacity, coordination, and interoperability requirements:

☐ ACS type and scope of communications, including number and composition of coordinating entities (e.g., federal, SLTT)

☐ ACS configuration (i.e., for central ACS, consider needs for supplemental coverage; for multiple ACS throughout the area, consider interoperability needs of multiple systems across sponsor hospital and auxiliary sites)

☐ Scope of patient care, such as transient care (testing) or permanent (beds) and number being treated, potential duration of stay, and other factors influencing care (e.g., global vs. geographically-confined event; acute vs. non-acute care)

☐ Site characteristics, such as proximity to the sponsor hospital, size, configuration (e.g., placement/proximity of logistics offices to ACS dispatch or nursing subunits), accessibility, existing infrastructure, and layout

☐ ACS staffing requirements, such as communications methods and need for training and orientation on communications equipment use and procedures

☐ Integrated facility systems (e.g., power; heating, ventilation, and air conditioning; building security, cameras, and locking systems; sprinklers and alarms; generators)

☐ Patient transportation services (e.g., EMS, transportation services to/from sponsoring hospital or other ACS)

☐ On-site dispatch and operator services

☐ On-site security services or law enforcement presence

☐ IT and requirements for secure information and data entrance, storage, and transfer (e.g., patient, healthcare, and diagnostic portals; telemedicine; video teleconferencing)

☐ Communications providers and protocols (early consultation to meet mission requirements)

[9] States and localities are using a variety of platforms to coordinate resources and share information. For instance, 911, PSAPs, and ECCs may use Computer Aided Dispatch (CAD) systems to coordinate law enforcement, fire, and EMS resources and response. Also, in large metropolitan areas, EMS may employ city, county, or region-wide hospital status systems that may integrate with the CAD to indicate the status of a hospital, or services/capabilities of that hospital and their present status.

[10] Site identification is the process of identifying potential sites whereas selection processes require a comparison across options to choose the most appropriate facility to meet ACS mission requirements, including communications.

ACS communications should meet nationwide emergency communications standards, with considerations for how to successfully **plan for and deploy operable, interoperable, reliable, resilient, secure, scalable, and redundant capabilities and systems.**[11] Following a determination of ACS requirements, communications coordinators should assess existing ACS communications and IT infrastructure, coverage, and capabilities for voice, video, and data to meet mission needs.

Operability

Ability to provide and maintain reliable communications functionality throughout the area of responsibility

Interoperability

Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized

Reliability

Ability to function in any type of incident, regardless of cause, size, location, or complexity

Resiliency

Ability to perform despite damaged or lost infrastructure

Security

Incorporating data, network, and systems protection best practices into incident communications and data sharing in compliance with data protection and privacy laws

If there are gaps in coverage or capabilities, communications coordinators should reach to their communications equipment and technology reserves, mutual aid partners, service providers and vendors, and the state or territory to supplement coverage and capacity for ACS voice, video, and data needs. If the ACS is in a remote or rural area or public safety resources are unable to supplement coverage, **coordinating entities may need to deploy transportable solutions** (e.g., cell-on-wheels, cell-on-light-truck, man-portable cellular systems). When selecting and deploying solutions to support or augment the network, coordinating entities should consider necessary requirements for range of communications reception, configuration set-up to accommodate anticipated number of simultaneous users, necessary primary and back-up power sources (e.g., primary source and back-up generators), processes for adding mobile devices to the network, needs for additional equipment, and the size and placement of the deployable device. In some circumstances, **federal assistance is available to states, territories, and tribes** through the FEMA's Disaster Emergency Communications (DEC) Mobile Emergency Response Support (MERS).

ACS systems will also need preemption and prioritization to ensure that the site's vital voice, video, and data circuits and other telecommunications services receive priority treatment and are able to connect. **Priority Telecommunications Services (PTS) provide essential provisioning for ACS requiring installation of new services.** More information on how to request installation **or restoration** of services for deploying initial ACS capabilities is provided on *Page 7*.

In addition to ensuring ACS communications interoperate with the sponsoring hospital's systems and/or patient/hospital portals, considerations need to be made for securely entering, storing, and transferring sensitive information. Those coordinating **ACS communications should work with IT and security personnel, such as the ITSL, to incorporate data (e.g., patient data, personally identifiable information, e-personal health information), network, and systems protection best practices and compliance with data protection and privacy laws,** such as the 1996 Health Insurance Portability and Accountability Act (often referred to as HIPAA). Considerations should be made to determine who will implement and manage secure ACS system and data transfer. Cybersecurity resources for ACS systems needed to support data entry, storage, and transfer are on *Page 8.*

Interacting with Service Providers when Planning Communications for the ACS

- ✓ Confirm the service provider of the chosen facility immediately following site identification to assess the facility's capabilities and coordinate service augmentation to meet ACS communications requirements; identify service gaps and coordinate additional coverage options with the vendor point of contact
- ✓ Leverage pre-existing relationships with service providers and vendors and keep close coordination with them on the need to prioritize restoration and provisioning services for the facility
- ✓ Determine vulnerabilities to capabilities and confirm contingency plans and support for redundant systems with vendors

[11] FEMA's National Incident Management System (NIMS) has established these as standard communications system features.

Military Sealift Command Hospital Ship USNS Comfort (T-AH 20), originally deployed on March 30, 2020, as an overflow hospital for non-COVID patients, was converted to a COVID treatment facility shortly after due to changing mission priorities; however, it was left virtually unused due to the establishment of the ACS at Javits Convention Center and was redeployed after three weeks. Credit: U.S. Navy

Anticipating Changes to Mission

Communications should be planned and executed to meet identified mission requirements with the caveat that changes in requirements are likely and planning and execution must be agile. Social and environmental factors may require the ACS to expand or reduce services, change the mission, or resolve unanticipated disruptions in service. Therefore, those coordinating communications should **consider challenges and solutions to ensure the scalability and redundancy of ACS communications systems.**

ACS Expansion[12] – Initial coordination and site assessments account for a certain patient capacity. If the area's patient load suddenly increases, the facility may need to expand its functional capacity and coverage, assuming space allows.

Expect the Unexpected

Those coordinating ACS communications should include contingencies in ACS deployment plans to anticipate potential need for scaling communications, mid-operation, such as increases in bandwidth for one- or two-way telehealth services or video teleconferencing

ACS Functional Shift – Health crises and other disasters change the way we interact and the actions we take, especially as a result of social distancing and quarantine and isolation policies. These changes may decrease risky behaviors among the masses, potentially reducing the need to treat an overflow of *non-afflicted patients*. However, increased demand for treating *afflicted patients* may overwhelm primary-care facilities within a short timeframe, requiring an ACS to treat those affected by the crisis or disaster instead. Shifts in treatment often result in changes to the facility's function, and thus, its communications requirements.

ACS Disruption – Assessments and requirements determination phases should consider strategies for ensuring reliable and redundant ACS communications and service restoration. If the nation is experiencing a health crisis during, or approaching, a natural hazards season (e.g., floods, inclement weather, fire, hurricane), especially in geographically susceptible regions, the likelihood of service disruption or outages increases significantly.

Reliable and Redundant Systems

What happens when the primary ACS communications system goes down? The effectiveness and functionality of the facility may become compromised, potentially endangering patients and personnel. Therefore, those coordinating and standing up communications should consider system requirements and redundant capacities, including:

- Wired telephone capabilities
- Cellular capabilities
- Two-way radios
- Amateur radios
- Deployable sites to add coverage/capacity
- Satellite telephones
- Wired data services
- Alternative power systems

Communications coordinators should **revisit and understand existing contingency plans when performing ACS facility assessments and determining communications requirements, and adapt them**, as needed, to account for alternate communications capabilities and procedures in the event of an outage or need for expansion.

[12] Considerations should also be made to potentially reduce ACS operations, and thus communications requirements, if the facility's actual patient numbers are significantly under original capacity estimates.

Telecommunications Service Priority Program

The Telecommunications Service Priority (TSP) program authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits. The TSP program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to NS/EP.

There are two primary uses for TSP: **provisioning** of new services and **restoring** existing services. **TSP provisioning services are particularly relevant to standing up an ACS** as they provide priority installation of new voice and data circuits. 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 essential provisioning. These simplified steps show the basic process for requesting provisioning priority:

1. Call the Priority Telecommunications Service (PTS) Center for instructions on how to submit the request
2. CISA will provide a TSP Authorization Code for each service or circuit to be installed, which will be provided to the service provider and then given to the service vendor
3. The vendor will confirm receipt of the TSP Authorization Code(s) with the TSP Program Office

Those coordinating ACS communications should also **check the enrollment of the sponsor hospital and confirm extension of TSP restoration services to its auxiliary facilities**. TSP Authorization Codes are valid for three years. The FCC requires all users revalidate their requirement for TSP every three years before expiration. Users should be aware that TSP restoration priorities must be requested and assigned before a service outage occurs.

For more information on TSP, please visit the CISA web site at https://www.cisa.gov/tsp or contact the PTS Center toll free at 866-627-2255, 703-676-2255, or via email at support@priority-info.com.

ADDITIONAL CONSIDERATIONS FOR DECONTAMINATION AND DEMOBILIZATION

ACS communications operations should consider protocols for cleaning and disinfecting equipment, to include detailed guidance on frequency and cleaning/disinfecting procedures. Equipment and surfaces should be cleaned and disinfected as soon as possible after a known exposure; "high touch" surfaces and issued handheld equipment should be cleaned and disinfected before each shift or following each person's use. For more information, please refer to *CISA's Guidelines for 911 Centers: Pandemic Cleaning and Disinfecting*.

In anticipation of a decreased need for ACS as the public health need diminishes, those coordinating, managing, and operating ACS communications should implement a demobilization plan—ideally developed well in advance of the demobilization phase—including establishing a threshold for when demobilization will occur with ACS Operations Managers. Once demobilization determination has been made, the following steps should be taken:

☐ Ensure equipment is decontaminated in accordance with manufacturer guidelines, CDC guidance, and recommendations coming out of the United States Environmental Protection Agency regarding cleaning solutions, application methods, contact time, and surface use (i.e. particular surfaces require specific solutions) and conduct necessary maintenance

☐ Restore facility to its normal operating condition, including cleaning and disinfecting equipment or supplies utilized for the ACS mission

☐ Return equipment/supplies to regular location; conduct an inventory, and restock any depleted supplies

☐ Reassign staff according to current identified staffing needs in the jurisdiction

☐ Conduct an after-action review and collect lessons learned

☐ Review and update existing ACS communications plans, CONOPs plans, and pandemic plans, as necessary

CYBERSECURITY RESOURCES FOR ACS

The following resources provide information on cybersecurity that can be applied when constructing ACS:

Reports surfaced April 2020 of state-backed hackers breaching health care systems in the fight against COVID. Source: Federal Bureau of Investigations

- USACE
  - Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX) – CSC-MCX maintains state-of-the-art cybersecurity technical expertise and provides expert-level support to external stakeholders on a cost-reimbursable basis
- CISA
  - CISA Insights – Regularly updated website informed by cyber intelligence and real-world events, providing background information on particular cyber threats and the vulnerabilities they exploit, as well as ready-made mitigation activities to implement
  - Cyber Essentials – A guide that assists in developing an actionable understanding of where to start implementing organizational cybersecurity practices. The information is intended to help build a culture of cyber readiness comprised of six elements: yourself, your staff, your systems, your surroundings, your data, and your actions under stress
  - Interoperable Communications Technical Assistance Program – No-cost instruction and assistance designed to help emergency responders continue to communicate during disasters or large-scale planned events
  - United States Computer Emergency Readiness Team (US-CERT) – A program that provides timely, actionable cyber and communications information to increase understanding of how to mitigate threats and vulnerabilities; recommended actions to improve cyber risk posture; and recommended responses to attacks on both government and private sector networks. Subscriptions are available to several products including current activity, alerts, bulletins, tips, and analysis reports related to security issues, vulnerabilities, and exploits
- HHS
  - Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry – A report that addresses challenges facing the health care industry when securing and protecting against cybersecurity incidents, whether intentional or unintentional
  - Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients – Four-volume publication in response to a mandate set forth by the Cybersecurity Act of 2015 Section 405(d) to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry. It is intended to provide voluntary cybersecurity practices to healthcare organizations of all types and sizes, ranging from local clinics to large hospital systems
  - Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information – A guide designed to help health care providers better understand how to integrate federal health information privacy and security requirements into their practices
  - Working Without Technology: How Hospitals and Healthcare Organizations Can Manage Communication Failure – A fact sheet offering recommendations for healthcare organizations and facilities on how to alleviate issues associated with a breakdown in traditional forms of communication
- DHS
  - Cybersecurity Strategy – A department-wide risk management approach and framework for improving the security and resiliency of cyberspace. The strategy is based on five pillars: risk identification, vulnerability reduction, threat reduction, consequence mitigation, and cybersecurity outcomes enabling
- Journal of Medical Internet Research
  - Cybersecurity in Hospitals: A Systematic, Organizational Perspective – An article discussing several key mechanisms that hospitals use to reduce the likelihood of cybercriminal activity, including reducing end point complexity and improving internal stakeholder alignment
- National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework – A framework consisting of standards, guidelines, and practices to promote the protection of critical infrastructure. The approach is prioritized, flexible, repeatable, and cost effective to assist owners and operators of critical infrastructure to manage cybersecurity-related risk