Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY

MANAGEMENT CHECKLIST FOR TELEWORKING SURGE DURING THE COVID-19 RESPONSE

MARCH 2020

Management Checklist for Teleworking Surge During the COVID-19 Response

While teleworking has become a routine way of doing business in many industry sectors and government, teleworking during wide-scale public emergencies such as what we are experiencing with the emergence of the COVID-19 virus introduces significant management, technology and bandwidth challenges to ensuring uninterrupted and efficient workflow and provision of services to the public. Added strain on the public telecommunications infrastructure over the “last mile” to the home, in particular, requires critical healthcare entities to assess risk, prioritize tasks and apportion bandwidth resources to ensure continuity of mission-essential functions that may migrate off premises to the home office environment.

This checklist is designed as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and I.T. security, and supply chain resilience.

About the Health Sector Coordinating Council Cybersecurity Working Group

This checklist was developed by the Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector’s ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 300 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Disclaimer

This document is provided for informational purposes only. Please note that the information presented may not be applicable or appropriate for all health care organizations, nor is it intended to be an exhaustive or definitive source on teleworking as a result of COVID-19. The first three pages consist of a checklist followed by detailed information and resources.

Recommendations Checklist

Information Technology - Teleworking

I. Bring Your Own Device (BYOD) Policy
   a. Suggest reevaluating BYOD polices for individuals that do not have company issued laptops to adjust the rules if the need arises for remote work.
   b. Suggest use of mobile devices for email and critical functions. Assess two/multi factor[i] authorization implementation.

II. Cloud Providers
   a. If using interim cloud solutions to augment telework ensure the workload is appropriate for the cloud and Backend-as-a-service (BaaS) are in place where ePHI may be handled.
   b. Verify cloud-based services restricted to an organization's IP range is accessible via the VPN.
   c. Ensure proper lines of communication exist between the cloud provider and the organization.
   d. Ensure proper monitoring of the cloud provider is in place.
      i. Monitor usage and validate against any service or licensing limits, performance impacts, security events and costs/plans for potential overages with financial teams.
   e. When possible, ensure federated access is in place between the cloud provider and any federated sign-in portal. Verify the portal is accessible via the VPN.

III. Cybersecurity[ii]
   a. An increase in remote work can increase the risk for business email to be compromised, distributed denial-of-service (DDos) and malware and phishing attacks.
   b. Suggest creating and monitoring Intrusion Detection System (IDS) filters and encourage regularly changing passwords.

IV. Data Centers
   a. Assess remote access and bandwidth usage to support an increased number of remote employees.
   b. Ensure entry and exit procedures exist for data centers and increase cleaning frequency of equipment.

V. Network rationing
   a. Review employee work hours and consider staggering hours of operations to ease bandwidth demands. Assess the upload rate to cloud and adjust to meet the bandwidth restrictions.

VI. Security/Network/Telephone Operation Center Management
   a. Multi-connectivity options for key support personnel: Software VPN, Hardware VPN, VDI.

VII. Telemedicine
   a. Subscribe to broadband service for high-speed data transmission.
   b. Desktop computers and mobile devices selected for telemedicine purpose should be encrypted with software and hardware that is HIPAA compliant.

VIII. Third Parties
   a. Contact critical suppliers in effort to understand their exposure, risk mitigation plans and overall situation readiness.

IX. Virtual Private Network (VPN) and Virtual Desktop Interface (VDI)
   a. Ensure enough company licenses for VPN connections and consider rules to allow for bandwidth to be freed. Consider user population that may need access in urgent circumstance.
   b. Implementing access prioritization by creating separate URLs for high priority users vs general users.
   c. Assess bandwidth quality of service dependent upon what type of activity/application the user is working on.
   d. Consider implementing split tunneling capability for a better user experience and lessen VPN usage.
   e. Transition remote patching schedules to off-hours (evenings, weekends) or consider deferral, if needed. Review if it will require the user to initiate the download and restart.

X. Videoconferencing
   a. If conditions dictate that it is necessary, communicate that it is recommended to use video only when necessary. Encourage the use of voice and chat communications

Legal and Privacy Considerations

I. Review HIPAA Privacy and Security for telemedicine[iii] to ensure legal and compliant practices.

II. Understand and consider insurance coverage for Malpractice and Cyber to ensure safeguards when transitioning to increased amount of remote work.

III. At home, consider the legal and privacy of any PHI that you will have access to in a remote environment.

IV. If applicable, review the Telemedicine Interstate Medical Licensure Compact [iv]

Communication[v]

I. Ensure enhanced communications plans are developed and renewed in training employees unaccustomed to telework.

II. Ensure availability of a mass notification system (calls, text, personal email, etc.) to communicate critical/urgent messages to staff across various areas.

Preparing in the Workplace

I. If you have hot desks at work, common in the IT workspace, ensure extra precaution in cleaning desktop surfaces and shared IT equipment.

II. Executives and business managers should identify critical sets, or positions where they may not be any additional labor to perform the function. Define critical positions[vi] for your organization.

III. Review cleaning schedule and that you have proper cleaning equipment available in your work space.[vii]

Preparing at Home[viii]

I. Medical Devices: Review mechanisms for managing/cleaning/disinfecting infected patient devices. All patient devices that may have been exposed to an infected patient need to be cleaned according to manufacturer's guidelines. These are always available on their manufacturer website.

II. Higher security vulnerability for devices at the home
   a. Identify all connected devices in the home

b. Patch vulnerable devices (including firmware)

c. If your ISP provided a modem and router in one device, add a commercial grade wi-fi ethernet router and network firewall

    i. Change default settings and passwords (use strong, long passwords)

    ii. Use the strongest wireless encryption protocol available (Wi-Fi Protected Access (WPA 3) is preferred)

    iii. Disable Wi-Fi Protected Setup (WPS)

    iv. Turn off Universal Plug and Play (UPnP) and other router features you don't use

    v. Disable remote management

    vi. Disable PING, Telnet, SSH, UPnP and HNAP on the router if possible, by setting the ports to "stealth"

    vii. Use two-factor authentication where possible

    viii. Change the default service set identifier (SSID) so the network name does not reveal the device manufacturer, your location or identity

    ix. Isolate work devices from non-work devices – create a dedicated work segment and two or three other segments (this is especially important if vulnerable devices can't be patched). Be sure to properly secure all network segments, including guest.

    x. Use the 5-GHz band to reduce wireless signal distance so it does not propagate beyond the perimeter of your home

    xi. Change the home router DNS server from the ISP to the enterprise standard DNS or a secure DNS server if no standard exists

    xii. Change the router's default LAN IP address and enforce a secure HTTPS connection over a non-standard port to access your router's administrative web interface

    xiii. Require a VPN when connecting from the home to enterprise network with strong authentication (not just passwords), strict authorization and access controls

    xiv. Turn off the network when it is not in use

    xv. Monitor for unknown device connections

    xvi. Pay attention to vulnerable IoT devices on non-wifi protocols such as ZigBee and others, since these have also been used as attack vectors to compromise computer networks in homes

Supplementary Detailed Information

Information Technology - Teleworking

I. Cloud providers
   a. Ensure proper monitoring of the cloud provider is in place.
      i. Monitor usage and validate against any service or licensing limits, performance impacts, security events and costs/plans for potential overages with financial teams.

II. Telework may cause a surge of cloud service usage. Review any limits in place.
   a. Validate potential licensing limits associated with additional usage.
   b. Understand and validate any technical service limits.
   c. Validate resource are properly sized and consider scaling services up in anticipation for a surge of usage.

III. Ensure proper lines of communication exist between the cloud provider and the organization.
   a. Inform any account manager or customer success manager of the potential for increased service usage demand.
   b. Verify IT staff has access to all channels for support

IV. Identify SaaS solutions that may not require VPN access.
   a. Remind employee's that interim collaboration solutions adopted for improved telework communications require review by the IT department

V. Telemedicine
   a. Consider investing in imaging and peripherals devices, having redundant systems available, planning for enough storage to maintain system availability and for data backups.

VI. Legal
   i. Professional Licensure
      1. Default rule (~48 states): A practitioner providing services via telehealth must be licensed in the state where the patient is located.
      2. Certain exceptions are recognized
      3. ~15 states have special-purpose telemedicine licenses
      4. ~28 states allow for infrequent or occasional consultations
      5. Interstate Medical Licensure Compact (IMLC): Currently, 29 member states (plus the District of Columbia and the Territory of Guam) have signed on to this voluntary, expedited pathway for physicians seeking to practice in multiple states. [https://imlcc.org/]
      6. Does the practitioner meet the IMLC's eligibility requirements? According to the IMLC, approximately 80% of physicians meet the eligibility criteria. [https://imlcc.org/do-i-qualify/]
   ii. Documentation
      1. How will the practitioner validate the patient's identity before providing treatment via telehealth?
      2. The flip-side is: How can the practitioner best preserve the telemedicine patient's confidentiality and anonymity vis-à-vis other parties?

3. How will the practitioner obtain the patient’s informed consent before providing treatment via telehealth?
4. Record keeping: How will the practitioner maintain clinical materials generated via telemedicine? Will screenshots or video recordings be incorporated into the patient’s electronic medical records (EMR)?
    a. Via a patient portal or mobile app?
    b. Is it secure / encrypted?
    c. Is it HIPAA-compliant (e.g., Will the vendor sign a BAA?)

iii. HIPAA Privacy & Security

1. HIPAA provides a floor re: safeguards, but states may enact stronger security, privacy, and breach notification provisions.
2. Telemedicine providers must maintain all appropriate documentation:
    a. Business Associate Agreements
    b. Patient Informed Consent Forms
    c. Patient Rights for Telehealth Encounters Forms

iv. Insurance Coverage

1. Malpractice Insurance
    a. Does the practitioner’s malpractice insurance cover the services that are being provided via telemedicine?
    b. Does the practitioner’s malpractice insurance coverage apply in every state where the patients being treated via telemedicine are located?

v. Cyber-Insurance

1. Does the practitioner have cyber-insurance?
2. Medical Billing and Reimbursement?
3. Place of Service (POS) code
4. Individual clinicians may need to change POS code - that is the "place of service". If the services are being delivered 100% from home, then the clinician's home address should be used. However, if this is a temporary measure for pandemic business continuity, it may be permissible to keep the clinic as POS. Clinician needs to check with the provider's MAC. In some regions, if the clinician has assigned their billing rights to a group or facility, that group/facility address may be the POS, regardless of whether the provider is seeing patients from his/her home.

Communication

I. Ensure enhanced communication plans are developed

a. Encourage organization-wide policies for telework

b. Ensure consistent information to all employees are aligned with goals of the organization

c. Any clarification regarding guidelines should be addressed with your supervisor.

d. Positive working relationships depend upon mutual understanding of goals and objectives, encourage employees to raise concerns as the potential in job responsibilities during the process may be adjusted. Consider quick video updates from employer leadership team as conditions evolve.

II. Ensure backfill plans for illness-displaced skills sets
   a. Follow policy for reporting illness, request time off
   b. Ensure departments have up to date job descriptions and consider a common weekly project report out format, in the unfortunate event back fill needs to occur
   c. Create opportunity for well employees to volunteer to cover co-workers who might be out with illness by providing clear messaging for needs.

III. Meetings: capacity, time, video, phone, etc.
   a. Adopt policies discouraging non-essential travel
   b. Follow normal scheduling practices for online meetings
   c. Encourage use of video for meetings, supporting transition of new remote working
   d. Consider procedure to take minutes or establish mechanism to receive consent for recording meetings for illness-displaced individuals to review later

IV. Renewed training/guidance for employees unaccustomed to telework
   a. Ensure each employee has access to remote work capabilities, including shared servers and video conferencing
   b. Keep lines of communication open
   c. Training on work/life balance (know when to get out of the house)

V. Mass Notification System
   a. Ensure availability of a mass notification system (calls, text, personal email, etc.) to communicate critical/urgent messages out to staff across various areas.
   b. E.g. facilities, regional and organizational levels

Preparing in the Workplace

I. Assessing Critical Personnel
   a. Executives and Business managers should identify critical skill sets, or positions where there may not be any additional labor to perform the function, and establish a practice of isolating the individual/s performing the work to reduce the possibility of exposure
   b. Critical positions standards include but are not limited to the following.
      i. Obligates, expends, collects or controls revenue, funds or items with monetary value in excess of $50 million.
      ii. Procures (or secures funding for) goods and/or services with monetary value in excess of $50 million annually, with the potential for devastating impact on an organization's programs or operations.
      iii. Significant, independent responsibility for the disposition, handling or transportation of hazardous materials, with the ability to circumvent procedural, physical and oversight processes.
      iv. Develops/directs/ implements/administers computer security programs, including risk analysis/threat assessment without technical review.
      v. Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware or software.
      vi. Automated access to a system during operation or maintenance or preparation of data for entry into a computer system in any way that creates high risk for causing severe damage or realizing significant personal gain (for example, the ability to independently manipulate data)

Resources

COVD-19 Information

- CDC COV-19 Situation Summary
- CDC About the Disease COVID-19
- John's Hopkins COVID-19 Tracking
- WHO COVID-19 Information
- McKinsey COVID-19 Implications for Business

Pandemic Preparedness

- CDC Pandemic Preparedness
- Gartner the Pillars of Pandemic Planning
  - ○ the-pillars-of-pandemic-planning.pdf
- HHS/CDC Business Pandemic Influenza Planning Checklist
- ISSO 22301 – Business Continuity

Information Technology

- Cybersecurity & Infrastructure Security Agency (CISA) Updates on COVID-19
- CISA Insights Risk Management COVID-19
  - ○ CISA Insights - Risk Management for Nov
- NIST Publish Multifactor Authentication Practice Guide
- WHO warns of Coronavirus Phishing Attacks

Legal and Privacy

- HIPAA Privacy and Novel Coronavirus
  - ○ february-2020-hipaa-and-novel-coronaviru
- Interstate Medical Licensure Company

Communication

- CDC Communication Resources for COVID-19
- CDC Travel Information for COVID-19D
- Pan American Health Organization Pandemic Communication Plan Tool Kit
  - ○ RespToolKit_21_Tool 13_CommunicationsPl

Preparing at work

- CDC interim Guidance for Business and Employers to Plan and Respond to COVID-19
- CDC – Risk assessment of Persons with Potential COVID-19
- DHS – How to disinfect your workspace
- DHS – Proper Handwashing
- WHO - Getting your Workplace Ready

Preparing at home
• CDC Preparing at home

ENDNOTES

[i] NIST Publish Multifactor Authentication Practice Guide

[ii] Cybersecurity & Infrastructure Security Agency (CISA) Updates on COVID-19

[iii] HIPAA Privacy and Novel Coronavirus

february-2020-hipaa-and-novel-coronaviru

[iv] Interstate Medical Licensure Company

[v] Pan American Health Organization Pandemic Communication Plan Tool Kit

RespToolKit_21_Tool 13_CommunicationsPl

[vi] Gartner the Pillars of Pandemic Planning

the-pillars-of-pandemic-planning.pdf

[vii] WHO - Getting your Workplace Ready

[viii] CDC Preparing at home

##