1. **Backup, Backup, Backup!**
   1. Have good daily backups. Ransomware infections continues to be a threat. Ransomware is when a user clicks on a phishing email and deploys malicious software onto their computer. The malicious software then “locks” any files that it can access. The Attacker then demands a “ransom” to unlock the files.
2. **Clearly Communicate Security Expectations of Remote Staff:**
   1. Have strong employee/end user agreements/rules on what type of work can and can’t be done at home.
   2. Include data handling in your employee agreements regarding how to treat sensitive and regulated patient information at home. (i.e. printing, shredding, and securing documents at home).
   3. If technically possible restrict employees from printing from home.
   4. If technically possible restrict employees from being able to save corporate and / or patient information on their local home hard drives and removable media like USB drives.
   5. If technical restriction is not possible include this in your employee agreements.
   6. Communicate to employees exactly what they should do if they discover that they have fallen victim to a phishing attack. Who should they call? Should they disconnect their computer from the Internet?
3. **Provide Training/Refresh Security Awareness Training**:
   1. Free online training or paid premium training is available online. See handout of links.
   2. Alert employees to increased phishing and social engineering attempts. The Bad Guys are not taking a break during the COVID 19 event.
   3. Remind employees not to click on links or open unexpected attachments.
   4. Ensure employees secure/use encryption for their Wi-Fi router at home. More information can be found at this link <https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network>
   5. Free Video on Creating a [Cybersecure Home](https://cc.sans.org/courses/a2a12ff3-5ea0-4898-bada-475a68f7366c/0/courseware.html?actor=%7B%22name%22%3A%5B%22Preview%20Actor%22%5D%2C%22mbox%22%3A%5B%22mailto%3Apreview%40test.com%22%5D%2C%22objectType%22%3A%22Agent%22%7D&endpoint=https%3A%2F%2Fcc.sans.org%2FScormEngineInterface%2FTCAPI%2F&process=false&auth=Basic%20Og%3D%3D&content_token=95c28679-231e-4a1b-ae72-c710dfdd24bc&activity_id=https%3A%2F%2Fwww.sans.org%2Fxapi%2Fcourses%2FMod129&externalConfiguration=&grouping=https%3A%2F%2Fwww.sans.org%2Fxapi%2Fcourses%2FMod129&content_endpoint=https%3A%2F%2Fcc.sans.org%2FScormEngineInterface%2FTCAPI%2Fcontent%2F)
4. **Verify Money Movement Requests:**
   1. All money movement requests for Direct Deposit changes, changes to vendor payment accounts, requests for wire transfers should be verified by phone.
   2. Do not trust email requests for money movement.
   3. Review/reconcile bank accounts daily.
5. **VPN/Encrypted Connections:** 
   1. Use a VPN for secure/encrypted communication between your network and the employee’s home PC. Make sure all VPN hardware/software has been patched/updated.
   2. Monitor all remote connections to your network. If possible set an alert for remote connections, otherwise review a daily report of remote connections.
6. **Multi-factor Authentication:**
   1. Implement the usage of multi-factor authentication for all remote access to your corporate network and any cloud services you use.
   2. If you are unable to implement MFA, move to a strong password (12-15 characters, numbers, symbols)
7. **Ensure Home Computers are “Healthy”**
   1. All home computers should be using a supported operating system (i.e. Windows 7 is now an unsupported operating system and does not receive security updates).
   2. Ensure employee remote equipment is set to apply all security patches automatically.
   3. Ensure employee remote equipment is running an antivirus software and that it is automatically updated.
   4. Ensure employee remote computers are running a personal firewall.
   5. Microsoft offers free guidance on Windows 10 security <https://support.microsoft.com/en-us/help/4013263/windows-10-stay-protected-with-windows-security>
8. **Resources for Additional, Local CyberSecurity Testing, Risk Assessment etc.**
   1. Monarch ISC – Joe Kurlanski, joe@monarchisc.com
   2. Tyler Technologies - Cybersecurity Division Jim Macisso jim.macisso@tylertech.com