COVID-19 CHECKLIST: SECURING YOUR BUSINESS AND CLINICAL IT

APRIL 2021

The Cybersecurity and Infrastructure Security Agency (CISA) has created this cybersecurity checklist to assist your healthcare delivery organization in mitigating vulnerabilities and protecting against malicious actors. Hospitals and healthcare facilities are facing cyber-attacks of varied sophistication, including criminal networks and nation states. Implementing these protocols, and instilling a culture of digital vigilance, will allow your team to focus on COVID vaccine and overall patient care priorities instead of the consequences of a cyber-incident.

☑ IMPLEMENT STRONG PASSWORD PRACTICES

- Use long passwords. We recommend using a unique string of words that can be easily remembered.
- Use different passwords for all accounts including email and social media accounts.
- Ensure each staffer has their own unique username and password. **Do not share accounts**.
- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.

☑ USE TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password.

☑ PROMPTLY INSTALL PATCHES FOR YOUR BUSINESS AND CLINICAL IT SYSTEMS

- Once patches are available, quickly install onto the operating systems of your computers, mobile devices and databases. Unpatched systems pose unnecessary risks to your systems.

☑ HAVE A PLAN TO QUICKLY RESPOND TO CYBER INCIDENTS

- Despite following these practices, cybersecurity incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.
- CISA may be able to assist with incident planning and recovery. Contact central@cisa.dhs.gov; communications to this email are covered by information sharing privacy protections and will not be reported to regulators.

☑ SECURE REMOTE ACCESS TECHNOLOGIES

- Technologies deployed for remotely accessing hospital networks are among the most targeted by adversaries.
- Change default or guessable passwords and enforce two-factor authentication (2FA) for accounts on Virtual Private Networking (VPN) and Remote Desktop technologies.
- Ensure remote access technologies accessible from the Internet are fully updated to mitigate vulnerabilities.

☑ BEWARE OF PHISHING ATTEMPTS

- Phishing is a common attack where emails, texts, or other communication are sent to a person to entice them to provide their username and passwords, or to open an attachment that has destructive software hidden in it, or click a link that brings them to a website that contains malicious software.
- Protect yourself from phishing attacks:
  - If the content of a message seems unusual or out of the norm for the sender, or you do not recognize the sender, do not open an attachment or click a link until you have contacted the sender.
  - Don't click on links for emails in your junk email folder, even if they appear legitimate.
  - Take a second to review links and attachments before opening.
  - If you suspect a text or email to be a phishing attempt report it to the appropriate IT provider.

☑ GET YOUR STUFF OFF SEARCH (SoS)

- Tools like Shodan, Censys, and Thingful can help you understand which assets are directly exposed to the internet and present an easy target for adversaries.

If you are experiencing or suspect malicious cyber behavior, contact CISA at 888-282-0870 or central@cisa.dhs.gov.