TEMPLATE FOR HEALTHCARE CYBERSECURITY INCIDENT ACTION PLAN

Every healthcare facility Chief Executive Officer should have a documented plan for recovery from a cybersecurity incident in the facility where the ability to use computers and other information and patient care technology is or could be compromised.

Elements should include:

I. Alternate plans for internal and external voice and data communication:

A. departments should have one or more fax machines to send and receive paper orders and reports, and one or more portable radios.

B. departments should have access to envelopes and postage meters to send materials externally,

C. departments should have access to a transport pool for internal materials if telephone and/or fax machines are not functioning,

D. departments should keep a list of telephone and fax numbers of frequent business contacts for ordering, etc., and workers and consultants and recheck it for accuracy semi-annually,

E. departments should prepare and store forms they use for ordering, reporting or documentation similar to their computer reports,

F. explore a relationship with one or more local amateur radio organizations to be on-call for emergencies.

II. A plan for departments to exercise their recovery plans individually and with all other departments at least annually.

III. A security incident response and business continuity action plan for immediate notification of key internal and external personnel including Board members and your local FBI office Cyber Task Force (with whom someone in your facility should have already developed a relationship).

Also, U.S. CERT and for further analysis and healthcare-specific indicator sharing at the Healthcare Cybersecurity and Communications Integrated Center at HCCIC_RM@hhs.gov. Ideally, facilities should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup. Keeping an incident private and not reporting it can do more harm to your patients, facility and other facilities in the long run.

IV. The department(s) responsible for information and patient care technology and cybersecurity should:

A. continuously monitor the U.S. CERT website at https://www.us-cert.gov/ncas

for the most up to date information,

B. review ASPR TRACIE resources periodically for the latest information,

C. request an unauthenticated scan of your public IP addresses from DHS at NCATS_INFO@hq.dhs.gov.

The U.S. CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks,

D. keep the CEO or designee, other management and department workers informed on a timely basis (in writing if at all possible),

E, participate in government/private sector calls for the latest updates and share information when possible to help others.

F. follow the FBI recommended steps for prevention to include:

a. enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing,

b. scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users,

c. ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans,

d. manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should use them only when necessary,

e. configure access controls including file, directory, and network share permissions with least privilege in mind. If users only need to read specific files, they should not have write access to those files, directories, or shares,

f. disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications,

g. develop, institute and practice employee education programs for identifying scams, malicious links, and attempted social engineering,

h. have regular penetration tests run against the network, no less than once a year, and ideally, as often as possible/practical.

i. test your backups to ensure they work correctly upon use.

G. Follow FBI recommendations for defending against ransomware generally with these precautionary measures:

a. ensure anti-virus is up-to-date,

b. implement a data backup and recovery plan to maintain copies of sensitive or proprietary data in a sensitive and secure location. Backup copies of sensitive data should not be readily accessible from local networks,

c. scrutinize links contained in emails, and do not open attachments included in unsolicited emails,

d. enable automated patches for your operating system and web browser.

H. develop a plan for alternate treatment when patient care equipment has been compromised.

V. A plan for facility participation in a government/private sector partnership organization to keep current.

VI. A plan for consideration of cybersecurity insurance.