Staying Cyber Safe in the Healthcare and Public Health Sector
Tips for individuals and organizations

As cyber attacks on the Healthcare and Public Health Sector continue to rise and directly affect patient safety, it is important to know why healthcare is targeted and what you and your staff can do today to mitigate these attacks.

HHS 405(d)
Aligning Health Care Industry Security Approaches

Why is healthcare targeted?

1. Protected Health Information (PHI) and Personal Identifiable Information (PII) is worth a lot of money for attackers.
2. Ransomware attackers take advantage of the time sensitive nature of healthcare and rely on health organizations paying ransoms to continue delivering patient care.
3. The healthcare industry also encompasses outdated technology that is vulnerable to attackers.
4. Healthcare staff include a wide range of professions and not everyone is educated on cyber hygiene and safety.
5. Healthcare has a broad attack surface because of many connected devices that reside inside a small, medium, or large health organization.

Where do these attacks come from?

Organized crime and online criminals

These groups sell healthcare data due to its high monetary value and are active in holding systems and data for ransom.

Foreign actors and governments

These groups are interested in healthcare information that might give them a political advantage or insight into the American public.

Malicious insiders

These individuals use their access to an organization's data to perform malicious activity such as stealing PHI or PII for monetary gain.

Accidental and honest mistakes

These individuals make honest mistakes such as sending sensitive data through an unsecure email which leads to a data breach.

Cyber Hygiene Tips:

Identify and report email phishing attempts

When in doubt, report the email to your IT personnel. Never provide sensitive information when being asked in urgency. Always double check the source and, if needed, call the requester to verify.

Protect patient data

Always ensure you are protecting your patients' data by using encryption. Get to know your organization's policies when accessing and transmitting sensitive data. Also, be aware of social engineering techniques that ask you to email or mail patient information.

Secure all your IT Equipment

It is important to protect your smartphone, tablets, laptops, and computers both physically and remotely from threats. When you leave your device always lock it with a secure password and never leave it unattended. Also, it is important to never ignore software updates your organization pushes as they provide extra protections for your devices.

Use multi-factor authentication

Requiring more than one form of identification to validate users accessing your systems will provide a double layer of security.

Be cyber smart while working remotely

Be very careful when accessing your organization's network from a remote location. Hackers frequently intercept open Wi-Fi networks, which could leave your organization's network at risk. Therefore always use secure, password protected Wi-Fi. It's also best to always be connected through a password protected Virtual Private Network (VPN).

Report suspicious activity immediately

Whether you are noticing glitches in a database or you get a suspicious email, when in doubt report any suspicious activity immediately as this can prevent a cyber attack from spreading through your organization.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov or our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*