Identity Theft and Cyberattack Protections

HCMS Harris County Medical Society

Please note that the content provided herein is INFORMATIONAL only, and should NOT, in any way, be considered legal, professional, business, practice, nor other advice. Please consult your own adviser and/or attorney before taking any action or inaction based on this information and to also confirm that you are compliant with all applicable requirements and laws.

Data breaches and cyberattacks are on the rise in the healthcare industry costing the industry millions of dollars and placing physician practices at risk. This resource will offer just some items to consider in regards to identity theft and cyberattacks.

Identity Theft Protections:

Identity theft uses the personal or financial information of another person to commit fraud, such as making unauthorized transactions or purchases. Below are just a few practices that may help prevent identify theft:

- Credit freeze – Consider freezing your credit with the three major credit bureaus (Experian, TransUnion, and Equifax) if there is not an immediate need to have your credit run (you are not seeking a loan, applying for a job that requires a credit check, etc.). Freezing your credit is currently free, as opposed to locking it, and can be unfrozen when the need arises. For instructions and more information on freezing credit visit NerdWallet.

- Monitor credit and account activity – Frequently review credit reports from the three major credit bureaus. Also review regularly your banking, credit card, and other statements for suspicious transactions. If you see a suspicious transaction, contact your bank, credit card company, lending institution, financial institution or other applicable institution immediately and report it.

- Alerts – Consider setting up alerts to notify you of activity on your credit cards, bank accounts, websites, etc. Consider using a digital wallet (an app containing secure, digital versions of credit and debit cards).

- Passwords - Create strong and varied passwords or use a password generator. For password creation guidance visit the GFC Global resource.

- Encryption – Encrypt devices when possible. Only provide sensitive information on encrypted websites (look for “https” in the URL). For encryption instructions for various devices consult this guide.

- Antivirus software/firewall - Use security software like virus/malware protection applications, set up a firewall, and set the configuration to update automatically. Install a firewall between your internal network and the internet to help prevent unwanted internet access. Your router may also have a firewall; utilize it and make sure it is properly installed. If you use Microsoft Windows, enable its firewall as well (the firewall setting is typically located in the control panel setting).

- Multi-Factor Authentication (MFA) – Consider setting up MFA for any website or application that supports it. MFA will send a unique code to the person attempting to access your data to validate they have permission to log-in.

- Social Security Numbers - Do not provide your social security number unless necessary, and if necessary, see if you can only provide the last-four digits.

- Public Wi-Fi – Try to avoid using public Wi-Fi unless you can use a Virtual Private Network (VPN).

- Unsolicited calls, emails, messages - Do not give unsolicited callers any of your account or personal information or let them take remote control of your computer. Instead, validate the call by contacting the entity directly using their published phone number or the one listed in your account (not a phone number the unrecognized caller gave or emailed you). Do not click on links in unrecognized emails, texts, or social media, since these can be part of schemes used by hackers to gain entrance to your device. Instead, go directly to the source to verify the message was sent legitimately.

If your personal information has been exposed in a breach, in addition to the above, consider taking the following actions:

- Depending on the type of breach, contact your police department, submit an Identity Theft Complaint Form with the US postal service (if mail was involved), and notify the credit bureaus, banks, credit card companies, and lending institutions.

- Change all passwords, especially if passwords are repeated across various websites and applications, if they could have been exposed in the breach.

- Utilize the FTC guide and personal recovery resource and the IdentityTheft.gov guide.

- If a breach of your personal information occurred with an organization or business, consider taking advantage of the credit and/or identity theft monitoring and other resources offered by the organization or business.

Cyberattack Protections:

With cyberattacks on the rise, efforts should be made to ensure networks, ePHI, and other data are secure. Consider the following to secure your data and access to your systems:

- Firewalls - Install a firewall between your internal network and the internet to help prevent unwanted internet access. Your router may also have a firewall; utilize it and make sure it is properly installed. If you use Microsoft Windows, enable its firewall as well (the firewall setting is typically located in the control panel setting).

- Wi-Fi access – Many routers can facilitate more than one Wi-Fi network, such as a private one for staff and a public one for patients. Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID), which is the name of the wireless network, and only provide patients with the Wi-Fi login credentials on request. Do not use an identifiable name, such as “Dr. Smith’s Wi-Fi” for either the public or private network so as not to draw attention to your specific network. Also create strong passwords for both the public and private Wi-Fi networks.

  Also consider setting an access schedule for the public Wi-Fi. Within the router’s menu, time frames can be set to allow or disable internet access for network devices. For instance, if the office is closed on Sundays, access can be disabled on Sundays to keep people from using it.

- Wi-Fi hotspot - Your router may be a Wi-Fi hotspot for the office. Because of the importance of the router in the network, it should be protected with a strong password, which may not be the preinstalled password. If someone figures out your password, they can control the device, and monitor and record data passing through the router.

- Encryption - The public network can be accessed even outside the clinic's walls; anyone who has the SSID and password can connect at any time. When setting up the SSID, consider encrypting the Wi-Fi networks.

- Virtual Private Network (VPN) - VPNs create an encrypted tunnel for your data and protect your online identity by hiding your IP address. VPNs provide the ability to securely access your practice management and other systems using various devices like a tablet, PC, or a smartphone.

- Passwords – Require users to create strong passwords that use at least 8 characters (12 is better) and include numbers, upper and lower case letters, and special characters like $, %, #, @. Or use a password management tool to create strong passwords. Disable saving passwords to the browser. Enforce account lockout policies after a certain number of failed login attempts.

- Updates - Download and install software updates for your operating systems, programs, and applications as they become available.

- Multi-Factor Authentication (MFA) – Consider requiring MFA for any website or application that supports it. MFA will send a unique code to the person attempting to access your data to validate they have permission to log-in.

- Remote access tools – These tools present risk as they enable connectivity of two or more computers over a network or Internet connection that are on separate networks and/or in different geographical locations. Use paid versions of these technologies as they often have higher security and usually require multi-factor authentication and strong passwords.

- Printers/copiers - These devices can contain hard drives similar to computers and may automatically store a copy of every document that is printed or copied. Since these documents may contain protected health or other sensitive information, practices should ensure that the data stored on the devices' hard drives is removed or destroyed before the machines are disposed of or returned to the vendor if leased.

- Training – Train staff on the importance of system security and how to recognize threats such as phishing, email and web browsing scams, password protection, and other schemes used by hackers to gain entrance into the system.

- Backup systems - Hardware failure, natural disaster, and cyberattacks present a real threat to data loss and may expose the practice to HIPAA violations and fines, disrupt business operations, and require significant time, money, and resources to restore the data. Cyberattacks using ransomware are on the rise. This type of attack makes data unusable until a ransom is paid to the hackers. Having a current backup of the office data could potentially help to recover this information without having to pay the ransom fee or interrupt business operations. Develop and test backup and disaster recovery plans that anticipate how data may be lost and how to recover it. It is important that backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.

- Cybersecurity expert – Consider having a cybersecurity firm evaluate your firewalls, VPN, and other security measures to ensure they are working. Consider having the firm perform a real-time vulnerability test to uncover exploitable devices on the network. Also have the firm perform an annual penetration test to identify risks and expose weaknesses that might expose the system to a breach.

- Risk assessment – Consider performing a risk assessment annually, or have a cybersecurity firm do so, to evaluate how and where your system may be vulnerable to attack.

- Threat detection – Consider using Artificial Intelligence based threat detection technology known as Extended Detection and Response (EDR) software on all computers and servers. It is a consolidation of tools and data that provides extended visibility, analysis, and response across endpoints, workloads, users, and networks. EDR combines continuous, real-time monitoring and data collection with automated responses based on rules and analytics providing a centralized and integrated platform for data collection, correlation, and analysis, as well as for coordinating immediate threat alerts and responses.

- Cybersecurity Insurance – Consider adding business interruption insurance to existing policies and/or purchase a cyber liability insurance policy. Make sure coverage is available for a breach occurring outside of the practice such as a clearinghouse or other third-party vendor. Review the FTC Cyber Insurance guide to ensure the policy has the necessary coverage.

- Account maintenance - Audit accounts and disable unused and unnecessary accounts. Remove needless accounts that bad actors can leverage for entry into the system. Disable user accounts and access to organizational resources for departing staff.

- Apply the Principle of Least Privilege - Audit accounts with extensive or high-impact permissions (admin access) and remove any unnecessary permissions to reduce the damage that a bad actor can inflict through a compromised account. Avoid using admin user accounts for regular daily tasks. Regularly monitor usage of admin user accounts to detect unauthorized and malicious activity. Limit access to company data and information, and limit authority to install applications and software.

- Free resources - Review the National Coordinator for Critical Infrastructure Security and Resilience (CISA) ransomware guide and free cybersecurity services and tools for more information and resources.