Reporting Cyber Incidents to CISA

If you have been watching the news recently, Cybersecurity has been a huge issue. In the past few weeks:

- The FBI took down a Russian Bot Net Server that targeted the Internet of Things (IoT). The Internet of Things refers to devices connected to the Internet that are not computers or computer-related equipment including, but not limited to, doorbell cameras, home and office security systems, IV pumps, and any other device that can be controlled via an app on your cell phone.
- The U.S. and Germany took down a major server hub that sold stolen information, including stolen medical information.
- The U.S. Government has issued warnings that Russian hackers are likely to target computers and servers that are part of the U.S. infrastructure in response to the sanctions levied.

Medical identity theft is big business and the health information of people in the U.S. may be a high value target for Russian hackers. This means your data is at a much greater risk than it was just a few months ago. HIPAA regulations require us to take all reasonable precautions to protect our data and failing to do so is a HIPAA violation.

In addition, if you get ransomware and pay the ransom, you may be paying money to a country or organization that has been labeled a terrorist organization, which is a violation of the Patriot Act. Under this law, anyone who provides so-called material support to a designated terrorist organization **can be prosecuted**. Using this law, the Justice Department has convicted hundreds of Americans. (USA PATRIOT Act | FinCEN.gov)

This means you need to be even more vigilant in protecting your data than ever before. One of the ways we can prevent breaches and HIPAA events, and one way we can protect ourselves against fines from the federal government, is to share information when we experience an event, so others do not fall victim to the same type of hack or intrusion that invaded our systems.

To assist in that endeavor, the Cybersecurity and Infrastructure Security Agency (CISA) has published a fact sheet to assist with event reporting. (Sharing Cyber Event Information With CISA: Observe, Act, Report). This guidance document includes 10 key elements to share with the government, including:

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details
8. Severity of event
9. Critical Infrastructure Sector, if known
10. Anyone else you informed

We strongly advise you to download the document and keep it handy so you can become part of the collective shield that protects all medical practices from a cybersecurity event. This is truly a case where we can help ourselves by helping others.

TLD Systems assists practices of all sizes to implement strategies that will help avoid a cybersecurity event, with the goal of never needing to report a cybersecurity event in your practice. For more information, please contact TLD Systems.

Website: https://tldsystems.com/
Phone number: (631) 403-6687
Direct email: mbrody@tldsystems.com

Let the TLD Systems team be your resource to help YOU protect YOUR DATA.

Michael L. Brody, DPM