

Health Information Compliance Alert

Enforcement News: DHS Alerts Healthcare of Possible Iranian Cyber Attacks

As tensions escalate between the United States and Iran, the feds warn the healthcare industry and others to prepare for the possibility of cyber attacks.

The **Cybersecurity and Infrastructure Security Agency** (CISA), which falls under the **Department of Homeland Security** (DHS), cautioned that Iran may retaliate digitally against the U.S. as the country has been involved in previous data incidents.

"According to open-source information, offensive cyber operations targeting a variety of industries and organizations - including financial services, energy, government facilities, chemical, **healthcare**, critical manufacturing, communications, and the defense industrial base - have been attributed, or allegedly attributed to the Iranian government," said CISA in a Jan. 6 alert.

CISA recommends that IT professionals and vulnerable organizations take the following actions to cut down their chances of a data security incident:

- Step up monitoring and logging, including disabling unnecessary ports and beefing up protocols.
- Be aware of possible phishing schemes, particularly through emails.
- Stay on top of your patch management to shut the door on invaders.
- "Limit the usage of PowerShell to only users and accounts that need it, enable code signing of PowerShell scripts, and enable logging of all PowerShell commands," advises CISA.
- Back up everything and store at a safe and secure off-site location.

Read the alert at www.us-cert.gov/ncas/alerts/aa20-006a.