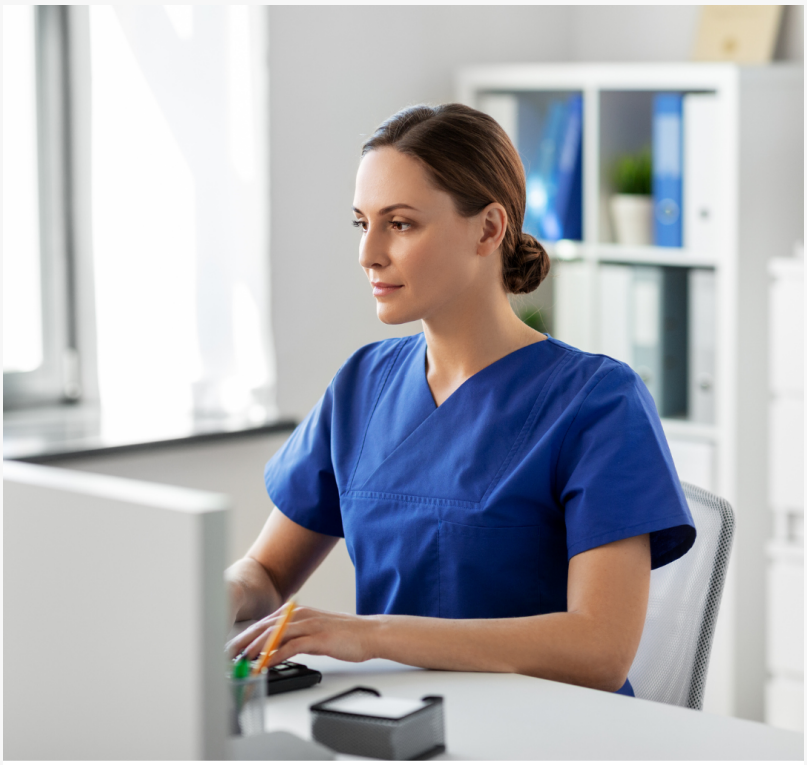
Healthcare Organizations are under attack now and should not wait for Federal mandates to enhance cybersecurity

The Healthcare Cybersecurity Act is still pending. Cyberattacks are increasing. Healthcare organizations should enhance their cybersecurity now.



SPOKANE, WASHINGTON, UNITED STATES, October 12, 2023 /EINPresswire.com/ -- The Healthcare industry is vulnerable to cyberattacks as all industries are, but the consequences could mean life or death.

Since January, 327 data breaches have been reported to the U.S. Department of Health and Human Services. The cyberattacks involved data of more than 40 million individual patients in 2023, making a 60% increase year-over-year for the first six months. Last year, a single breach involved two million records, but in the first half of 2023, there were five breaches of at least three million records each.[1]

Healthcare data breaches have doubled in three years, according to an IBM Ransomware study. In that period there was a 94% decrease in the time-to-encrypt, which is now less than four days.[2]

A ransomware attack on St. Margaret's Health, a small Illinois hospital, was a significant factor in causing it to close its doors permanently this year. There was no access to their IT system including email for four months.[3]

U.S. Senators Jacky Rosen (D-NV) and Bill Cassidy, MD (R-LA) announced they introduced their bipartisan Healthcare Cybersecurity Act, which would direct the Cybersecurity and Infrastructure Security Agency (CISA) to collaborate with the Department of Health and Human Services on improving cybersecurity in the Health Care and Public Health Sector, one of the United States'

> Healthcare providers need to be upping their game in cybersecurity and not wait for Federal regulations to mandate standards"
>
> *Heather Stratford, Drip7*
> *Founder and CEO*

sixteen critical infrastructure sectors.[4] The bill was introduced in 2022 and is still in the introductory phase.[5]

"Health centers save lives and hold a lot of sensitive, personal information, said Senator Cassidy M.D. This makes them a prime target for cyber-attacks," "This bill protects patients' data and public health by strengthening our resilience to cyber warfare."

According to JAMA, ransomware attacks on healthcare organizations are increasing in frequency and sophistication. Disruptions to care during ransomware attacks are an issue of patient safety and outcomes.[6]

Healthcare organizations are vulnerable to phishing attacks, ransomware attacks, data breaches, DDOS attacks (Distributed-Denial-of-Service attack), each is growing and has their own risk to both consumers of healthcare and to the providers.[7]

The Internet of Medical Things (IoMT). It's one of the top technological trends in healthcare for 2023.[8]

The 2023 State of Cybersecurity for Medical Devices and Healthcare Systems report finds that the software and firmware powering connected medical devices and healthcare applications are increasingly at risk due to numerous critical and high-rated vulnerabilities. The targeting of medical devices, software applications, and healthcare systems, found that 993 vulnerabilities–a 59% year-over-year increase from 2022–lurk within 966 medical products and devices, and attackers could exploit them to target a healthcare facility.[9]

"Healthcare providers must adapt to protect healthcare consumers, both their sensitive information in their records and patients receiving services. Those very medical records might also include critical information about a patient needed in a procedure or emergency treatment that could impact an outcome," stated Heather Stratford, CEO of Drip7. "Healthcare providers need to be upping their game in cybersecurity and not wait for Federal regulations to mandate standards."

"Unfortunately, the health care sector is uniquely vulnerable to cyberattacks and the transition to better cybersecurity has been painfully slow and inadequate. The federal government and the health sector must find a balanced approach to meet the dire threats, as partners with shared responsibilities," wrote Sen. Warner in the policy paper "Cybersecurity is Patient Safety."[10]

1. https://www.medicaleconomics.com/view/computer-attacks-in-health-care-are-booming-so-far-in-2023

2. https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf
3. https://www.darkreading.com/attacks-breaches/illinois-hospital-closure-ransomware-existential-threat
4. https://www.rosen.senate.gov/2022/03/24/in-light-of-russian-cyber-threats-rosen-cassidy-introduce-bipartisan-bill-to-improve-cybersecurity-in-healthcare-and-public-health-sector/
5. https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf
6. https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961
7. https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare
8. https://mapsted.com/blog/healthcare-technology-trends
9. https://h-isac.org/2023-state-of-cybersecurity-for-medical-devices-and-healthcare-systems/#:~:text=The%202023%20State%20of%20Cybersecurity,critical%20and%20high%2Drated%20vulnerabilities.
10. https://www.warner.senate.gov/public/index.cfm/2022/11/warner-releases-policy-options-paper-addressing-cybersecurity-in-the-health-care-sector

Heather Stratford is a national thought-leader in the Training and Cybersecurity fields. She is the founder and CEO of Drip7, a gamified microlearning platform for cybersecurity, compliance education and onboarding. She has started and exited several technology companies. Heather has written and been quoted in many media outlets, spoken at conferences, and been a trainer at events. She has consulted and spoken for multiple U.S. government agencies, State and Local governments, higher education, enterprise level businesses including fin/tech. Heather is a an Adjunct Professor at Whitworth University.

Deb McFadden
Drip7
+1 509-703-5400
PR@drip7.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
