BE CYBER SMART

Do Your Part. #BeCyberSmart.

CYBERSECURITY AWARENESS MONTH 2021

Welcome To Cybersecurity Awareness Month!

The theme for the first week of **Cybersecurity Awareness Month** is **"Be Cyber Smart."** The HHS 405(d) Program believes that means knowing about the top 5 cyber threats facing the healthcare and public health sector. In the past year, one of the most harmful cyber threats has been Ransomware. To learn more about Ransomware and how your organization can prevent this threat, check out the ***Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP).***

Current Ransomware Threat Against the HPH Sector

In 2020, the number of ransomware attempts against the healthcare industry rose by **123%**.

SonicWall Cyber Threat Report (2021)

In 2020, **92 individual ransomware attacks** affected **over 600** separate clinics, hospitals, and organizations and **more than 18 million patient records.**

Comparitech (2021)

Hackers demanded an estimated **$15.6m** in ransoms with an average of **$169,446** ransomware demand against U.S. healthcare providers in 2020.

Comparitech (2021)

18,069,012 individual patients/ records were affected by ransomware attacks in 2020— a **470%** increase from 2019.

Comparitech (2021)

Ransomware attacks cost the healthcare industry **$20.8 billion in downtime** in 2020, which is **double** the number from 2019.

Comparitech (2021)

The industry sectors that are currently experiencing the highest volumes of ransomware attack attempts globally are **healthcare,** with an average of **109 attack attempts per organization every week,** followed by the utilities sector with 59 attacks and Insurance/Legal with 34.

Check Point (2021)

Ransomware Attack Mitigation Practices to Consider

References in parentheses point to where you can find these practices within the HICP Technical volumes.

- Ensure that users understand authorized patching procedures *(7.S.A)*
- Use strong/unique username and passwords with multi-factor authentication (MFA) *(1.S.A, 3.S.A, 3.M.C)*
- Limit users who can log in from remote desktops *(3.S.A, 3.M.B)*
- Deploy anti-malware detection and remediation tools *(2.S.A, 2.M.A, 3.L.D)*
- Maintain a complete and updated inventory of assets *(5.S.A, 5.M.A)*
- Implement proven and tested incident response procedures *(8.S.A, 8.M.B)*
- Establish cyber threat information sharing with other healthcare organizations *(8.S.B, 8.M.C)*
- Develop a ransomware recovery playbook and test it regularly *(8.M.B)*
- Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures *(See the HHS Ransomware Fact Sheet)*