

SOLUTION BRIEF: HEALTHCARE DATA SECURITY SOLUTIONS

- Hospitals
- Healthcare Groups
- Healthcare Management



CHALLENGE:

Keylogging spyware is commonly downloaded as a result of clicking on an infected link and are often leveraged in a breach to steal network access credentials and other sensitive data. According to research, 71% of clinicians said their hospital allows some form of "Bring Your Own Device" (BYOD) to access hospital and patient information. Since this is often the same device they are using to access personal email, texts and social media, the BYOD employee poses an increased risk to keylogging spyware.

SOLUTION:

ACS EndpointLock Keystroke Encryption software eliminates the ability of keylogging spyware to capture keystrokes and steal access credentials to sensitive patient information. This includes doctors and staff who are accessing the network systems from their personal device. Hackers will always find ways to trick users into downloading a keylogger, but with EndpointLock installed, the spyware is rendered useless.

EndpointLock Benefits:

- Protection from Keylogging Spyware, the number one malware component.
- Protect Network Access Credentials.
- Protects the vulnerable gap found at the point of data entry.
- Runs in the background, no employee training needed.

DETAILS:

Health records are in high demand on the Dark Web because they contain all of a patient's personal information including name, address, birthdate, social security number, credit card information and medical records. According to a recent study published in the JAMA Network, phishing, poses a particular threat to healthcare organizations. Phishing is the practice of tricking unsuspecting victims into clicking on links that look legitimate. A recent Verizon Data Breach Report reported that phishing was found in 90% of breaches and 95% of all phishing attempts that led to a breach, were followed by software installation, including keyloggers. Keyloggers are typically used in the beginning stage of a breach to gain access credentials and other sensitive data. When a keylogger has infected a computer, tablet or mobile phone, it steals every keystroke typed into the device. Once network access credentials are obtained, hackers can either exfiltrate patient information or install ransomware to lock down the system and hold it for ransom in order to extort funds from the institution.

January 2018, HIPAA Journal:

The HIPAA Password Requirements and Best Way to Comply:

Accessing password-protected accounts from secondary devices increases the risk of a data breach due to **keylogging malware**. This type of malware runs undetected on computers and mobile devices, secretly recording every keystroke in a file for later retrieval by a hacker. As this is a foreseeable risk to the security of Protected Health Information, Covered Entities must either introduce policies to limit users to the devices from which they can access password-protected accounts, or find an alternative to the HIPAA password requirements."

NOTE: With 71% of healthcare professionals using a secondary device such as a mobile phone to manage their workflows, limiting their mobile use would be difficult.



SOLUTION TO HIPAA PASSWORD REQUIREMENTS

Installing EndpointLock keystroke encryption on all devices that are used to enter sensitive information such as passwords would address the vulnerability to keyloggers. Adding keystroke encryption will protect login credentials and patient data and fill a gap in endpoint security to protect the healthcare organization.

BEFORE

Hacker sends a phishing email



USERNAME: [REDACTED]
PASSWORD: [REDACTED]



Hospital Employee opens email and a keylogger is installed



Employee logs into the Electronic Health Records (EHR) network
USERNAME: [REDACTED]
PASSWORD: [REDACTED]

Employee logs into the Electronic Health Records (EHR) network

Hacker logs into corporate systems using stolen access credentials



AFTER

Hacker sends a phishing email



Hospital Employee opens email and a keylogger is installed



Keylogger is blocked by
EndpointLock™
Desktop and Mobile Security

USERNAME: [REDACTED]
PASSWORD: [REDACTED]



Employee safely logs into the EHR network.

Hacker is unable to retrieve any useful information, stopping the breach in its tracks

