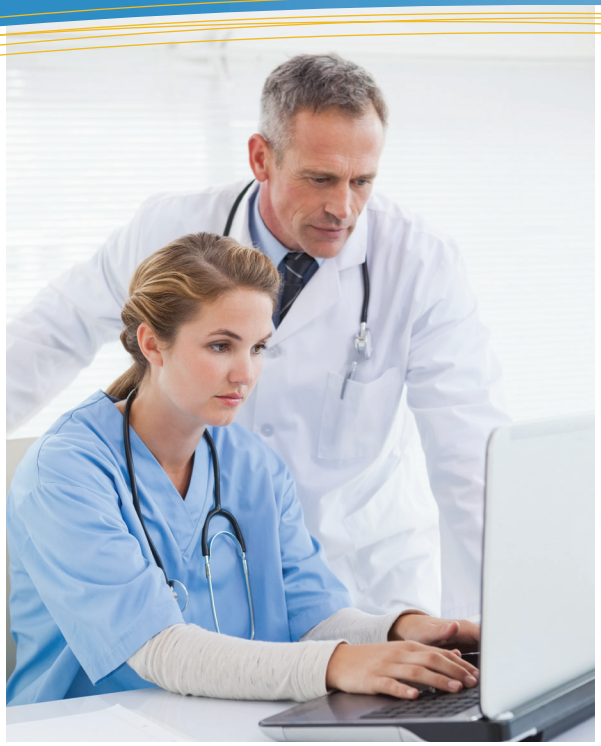
EndpointLock™

Spyware Protection Software

The most effective way to protect your medical practice from a costly data breach



- **Protection from spyware that is undetectable by antivirus and steals credentials & patient information**
- **Comply with HIPAA and PCI to avoid expensive breach penalties**
- **Encrypt keystrokes to protect EHR (Electronic Health Records) and medical billing**
- **Encrypt keystrokes to protect Patient PII (personal Identifiable Information)**
- **Encrypt and prevent spyware from capturing personal emails and texts**

Healthcare information is valued higher than credit card data on the black market because the personal information in health records never expire

Each year, healthcare organizations pay millions in penalty fees for losing EHR (electronic health records) and PII (personal identifiable information) to hackers. For instance, Anthem penalties have already exceeded 100 million in fees including the cost of issuing breach notifications to customers, paying OCR penalties, implementing new security measures and fighting lawsuits.[1] These kinds of fees can prove devastating to a small practice. Each violation will cost between $100 and $50,000, and then multiplied by the number of records leaked. For instance, if a practice has had 1,000 records leaked, the fine would run between $100,000 and $1.5 million, since the higher figure is the cap.[2]

According to recent reports, the majority of hacks involve stolen credentials [3], which are then leveraged in the initial stages of a healthcare breach in an effort to locate and steal EHR (electronic health records), and PII (personal identifiable information). Using various social and phishing techniques that cause the victim to unknowingly download an invisible keylogger to his or her device, these passwords can be easily stolen from even the most well-educated clinical or administrative employee. Keylogging spyware was at the helm of many of the biggest healthcare breaches of our time including the Anthem breach, which stole the personal information of over 80 million patients and Premera which stole over 11 million patient records [1].

The security solution for a BYOD world

COMPLIANCE CALLS FOR STRONG DATA ENCRYPTION AND THE SAFEGUARDING OF PASSWORDS

HIPAA (Health Insurance Portability & Accountability Act

PASSWORD MANAGEMENT (A) § 164.308(a)(5)(ii)(D):
"Implement procedures for creating, changing, and safeguarding passwords. "

TRANSMISSION SECURITY § 164.312(e)(1):
"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

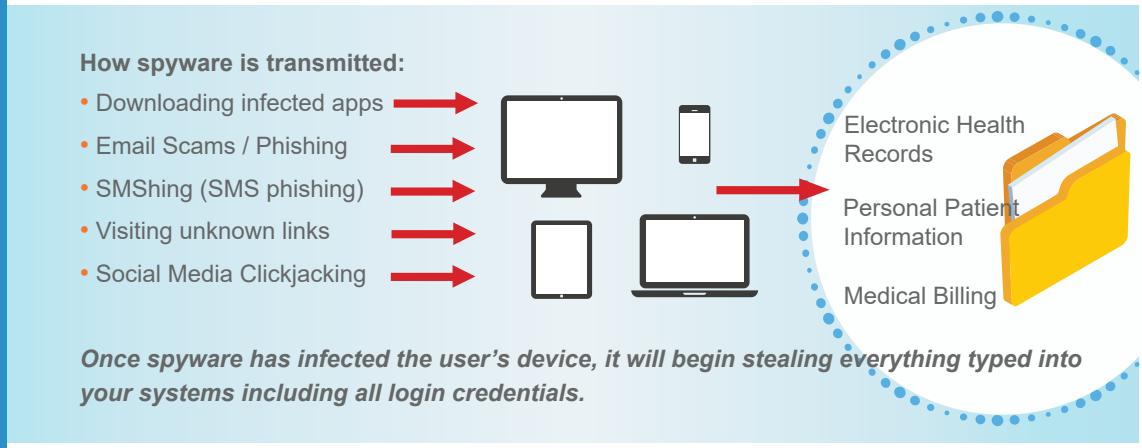
ENCRYPTION (A)§ 164.312(e)(2)(ii)
"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

PCI (Payment Card Industry) Security Standards Council

8.2.1: Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

With close to 85 percent of healthcare professionals using the same device for both personal and professional use, the likelihood for downloading malware increases exponentially.[4]

The bring-your-own-device (BYOD) movement in the workplace has proven to be extremely beneficial for the healthcare industry, allowing providers to readily access patient data, billing information, and office information very easily. Data now resides on desktops, laptops, smartphones, tablets and USB drives. However, the convenience of BYOD comes with a cost; as keylogging spyware can infect the user's device using various methods (see chart below).



Once spyware has infected the user's device, it will begin stealing everything typed into your systems including all login credentials.

EndpointLock™ Solution: Encrypts your keystrokes

Encrypting your data files into storage is important, but even stored data can be compromised when login credentials are stolen. EndpointLock™ protects all of your keystrokes including login credentials, patient health information and medical billing from being captured by keylogging spyware, which is one of the most common components in a data breach. EndpointLock™ encrypts your keystrokes to stop threats at the front door, keeping your private data protected. In addition to protecting your practice, you and your employees can get ID protection when texting, emailing, banking, shopping online and entering any other personal information.

Key Features:

- **Prevents spyware from capturing screen shots of images and sensitive data**
- **Available for mobile or mobile SDK to secure your own app**
- **Compatible with PC, Mac, iOS or Android**
- **Easy to Install**
- **McAfee ePO compatible**

References:
1. Zdnet.com: Anthem data breach cost likely to smash $100 million barrier
2. MedPagToday.com: How much will a data breach cost your practice?
3. 2016 Verizon Data Breach Investigations Report
4. mhealthintelligence.com: The Impact of BYOD