ENJOY SAFER TECHNOLOGY®

KEEPING YOUR HEALTHCARE FACILITY SAFE

www.eset.com

Keeping your healthcare facility safe

How to enhance your electronic immune system

Protecting patients at a healthcare facility is as much the IT department's responsibility as it is the doctors'. Between 2012 and 2015, the number of EHRs stolen annually skyrocketed from 2.7 million to nearly 110 million. And with more than 17,000 medical records illegally accessed every day, this trend shows no signs of slowing. This isn't surprising considering the innumerable hardware and software vulnerabilities that exist today, paired with the fact that a single healthcare record is worth 10 times as much as a compromised credit card number.

The healthcare industry is among the most targeted in terms of cybercrime, and your role on the frontline of a facility's electronic immune system is more important than ever. Fortunately, there are effective measures you can take to stave off such assaults.

Weaknesses in Websites, Mobile Apps, and the Cloud

Not long ago, employee negligence was the largest security worry healthcare facilities faced. Today, the primary source of security breaches has evolved from accidental to intentional, making outside attacks on web, mobile, and cloud-based applications the primary concern. Criminal attacks are up 125 percent since 2010, eclipsing the threat of lost laptops. And the more rapidly technology advances, the more vulnerabilities continue to emerge.

High-profile hacks at Anthem and Premera Blue Cross have exposed the information of tens of millions of patients, proving that even the largest organizations aren't immune to network breaches. In fact, the healthcare industry is assailed by more DDoS attacks than all other industries combined. And with 35 percent of adult Americans planning on purchasing health and fitness technology in 2016, the quantity and availability of sensitive data has never been greater.

Many mobile apps have been developed using open-source software that contains easily exploitable algorithms. This reality caught the public eye in 2014 with the discovery of the pervasive Heartbleed bug, which revealed a vulnerability in the OpenSSL cryptography library and allowed for a staggering amount of supposedly secure information to be accessed.

1 Source: Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, 2015
2 Source: FierceMobile Healthcare: Consumer interest in fitness, health projected to spur robust smartwatch sales
3 Source: 2014 Ponemon: Fourth Annual Benchmark Study on Patient Privacy and Data Security

Inadequacies in the Internet of Things

Beyond weaknesses on the web, new healthcare threats are emerging in the burgeoning Internet of Things (IoT). Many modern medical devices include Bluetooth and wireless network capabilities. While this offers a tremendous benefit to patients and doctors, it also increases the number of potential attack surfaces.

Vulnerabilities in networked medical equipment such as pacemakers and radiation machines are steadily increasing, making it possible for cybercriminals to manipulate the way these devices work. It was this risk that led former U.S. Vice President Dick Cheney to have the wireless feature in his implanted cardioverter defibrillator deactivated in 2013. And while the FDA insists that device manufacturers do their part to limit these risks, healthcare facilities must also take certain measures to reduce their exposure.

What role does the government play?

The passing of HIPAA in conjunction with 2009's HITECH Act introduced a new set of mandatory precautions healthcare facilities must take to protect patients' information. This includes stipulations for multifactor authentication and antivirus software on system servers. Businesses that neglect these and other recent regulations may face serious consequences in the event of a breach.

ESET protects facilities of any size

ESET can help ensure that your network's information is not only protected by multilayer security, but is also instantly accessible in the event of an emergency. No matter the size of your operation or how many patients pass through your doors, we have a complete suite of tools to monitor and maintain every aspect of your facility's technology:

1. ASSESS YOUR SITUATION—Understand your current preparedness for an attack to properly identify and address your exposure to threats. ESET's Professional Services can provide you with a comprehensive analysis of your security by conducting a HIPAA-compliant audit that pinpoints your organization's vulnerabilities.

2. ENCRYPT EVERYTHING—Stay safe from HIPAA penalties by dramatically reducing your susceptibility to a breach. ***ESET DESlock+ Encryption*** implements top-tier encryption that protects patients' information while providing your facility with immunity from government penalties.

3. ENABLE TWO-FACTOR AUTHENTICATION—Implement staff use of a combination of passwords and mobile devices to access your network. ***ESET Secure Authentication*** is an easy-to-install solution that greatly limits your risks.

5 WAYS TO PROTECT YOUR FACILITY:

1. Assess your situation
2. Encrypt everything
3. Enable two-factor authentication
4. Defend your facility on all fronts
5. Lock down your data

4. DEFEND YOUR FACILITY ON ALL FRONTS—Guarantee compliance with the HITECH Act by ensuring your network offers complete endpoint protection and control. ***ESET Endpoint Solutions*** combine antivirus, antimalware, and antispyware programs, alongside a firewall designed to prevent unauthorized network access while also allowing lost or stolen devices to be remotely wiped.

5. LOCK DOWN YOUR DATA—Maintain strict control over your EHRs by regulating the data types that can be transmitted to or from your network. ***ESET Security for Microsoft SharePoint*** is a must-have tool for facilities that store data on Microsoft's popular SharePoint engine.

Start protecting your facility now

In today's world, every medical facility is a target for cybercriminals. Plan your security as if you have already been breached. And for the best prescription on the market, count on ESET's comprehensive end-to-end solutions to keep your facility's immune system strong. Learn more. Read ***The State of Cybersecurity in Healthcare Organizations in 2016*** report now.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®