ebook

Cybersecurity for HIPAA Compliance

Healthcare is one of the most targeted industries for cyber-attacks. Learn what you can do to keep your patient's information safe.

radius180
Managed IT Solutions

HIPAA and Healthcare

The Health Insurance Portability Accountability Act of 1996 (HIPAA) was created to protect the sensitive health information of clients. With the integration of technology into the healthcare landscape, the lives of clients and healthcare workers are made easier by the accessibility and continuity provided by technology. However, it can be the gateway to a HIPAA breach.

Despite the convience of digital records, they can be a major vulnerability as online records pose a particularly attractive target for hackers. Healthcare is consistently one of the most targeted industries in cybercrime. Why are doctor's offices and hospitals hit more? Continue reading to discover what you can do to prevent an attack.

radius180

Why Target Healthcare

Healthcare is targeted more than other industries due to the large volume of important information that is stored in their systems. This can include credit card numbers, private health information (PHI), and personally identifying information (PII) like social security numbers. Once accessed, hackers can sell this data on the dark web.

Due to the sensitive nature of this information, hackers can sell healthcare records for up to 10 times more than other stolen records. Not only is it more profitable for hackers, but it is more expensive for victims. The cost to fix this type of breach is about $408 per record. That is approximately 3 times more than other industries!

radius180

Vulnerabilities in Healthcare

Mobile Clinics

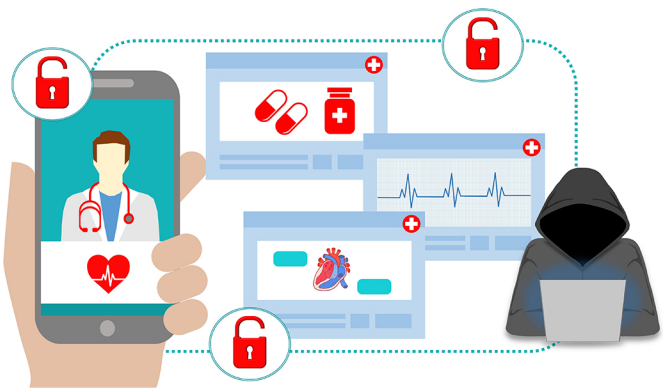
These clinics are great for providing services to a wider variety of people, but the lack of access to a consistently secure and known WiFi network can be dangerous. The constant use of different unsecured WiFi networks pose a serious cybersecurity.

Outdated Technology

Outdated security systems serve as an easy access point for those looking to exploit vulnerabilities. Failing to keep up with the newest secure technologies can come at a fatal cost.

Inadequet Staff Training

It is well known that the biggest risk to a company's cyber security are the humans that work there. Medical staff including doctors, nurses, and administrative staff must be trained on the risks specifically relating to digital records. Knowledge is most often the best defense against malicious hackers.



radius180

What You Can Do

1. Policy and Procedures

In the event there is a breach, it is imperative to have a set of response procedures. These procedures should be known by all employees. While you hope to never need to use them, having a plan in place will be invaluable in the event your office is compromised.

2. Education

One of the best actions that can be taken in order to prevent a cybersecurity attack is to educate workers on tactics used by hackers to compromise data and records. Through training, employees are able to more easily spot the top cyber-threats including phishing, cell phone use, password reuse and more.

3. Consult with Professionals

Meet with your current I.T. team or hire I.T. professionals who are expertly trained in cybersecurity. These professionals will audit your system for strengths and vulnerabilities. They will suggest changes and actions to best prevent cyber breaches.

radius180

The Next Steps

Don't lose your patient's information and trust in a HIPAA breach due to a cybersecurity attack. We'll help you take preventative measures. Do A 180 and contact us today.

For more information:
David Roberts CEO, Co-Founder

Phone: 856.282.1131 x101
Email: droberts@radius180.com

http://www.radius180.com

radius180