SVMIC

STRATEGIC

SERVICES

Cybersecurity Essentials

SVMIC provides resources for your cybersecurity programs. Access these through your Vantage® account.

SVMIC®

Cybersecurity Essentials

The threat to the security of electronic data is ever growing especially among the healthcare industry; thus, cybersecurity is a topic that should not be ignored. Many organizations tend to rely on weak and outdated systems and infrastructure. They may not have access to qualified IT professionals, or sufficient funding for cybersecurity programs may be lacking. Medical practices are a target for cyberattacks due to these weaknesses.

Security Risk Assessment

The foundation for any good cybersecurity program is a thorough Security Risk Assessment. These assessments catalog where ePHI is created, stored, received, and transmitted, what potential risks are associated with that data, and determine the probability of those risks and how detrimental those risks would be to the security of the data should the risk occur.

Security Incident Response

When the security of a healthcare entity's computer system is threatened, it is important for that entity's IT team to have a plan in place on how to respond to the incident and address steps to ensure similar incidents are reduced.

Data Backup

After conducting a Security Risk Analysis, a practice should have an inventory of all devices that house electronic patient data. Once this data is identified, the practice will need to determine what data backup services will be needed so that this data can be restored should the computer systems crash or come under attack. While cloud based EHRs are generally backed-up by the EHR company, data housed within the healthcare organization's own computers will need to be backed-up by the practice. Consult with a well-qualified IT professional to determine what data needs to be backed-up, how often it should be backed-up, and what type of backup system works best for the practice.

Security Technology

Technology is an important aspect in securing computer systems from inappropriate access. There are various technologies available to protect systems, including encryption, system vulnerability scans, and multi-factor authentication. Consulting with a well-qualified IT professional will assist the practice in determining which technologies are right for them.

Staff Education

Regardless of what hardware, software, and policies are in place to protect against cyber threats, if staff are not educated on how they can avoid some of these threats, these efforts may not be as effective. The need to access various websites or have access to email puts the practice at risk. Staff must be aware of the risks and how they can avoid them.

SVMIC's Services

SVMIC is dedicated to providing resources to our policyholders to assist in their cybersecurity programs. You may access these and other cyber resources online through your Vantage® account. If you have questions about cybersecurity, call 800-342-2239 and ask for Medical Practice Services or email ContactSVMIC@svmic.com.

If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and asking to speak to the Claims Department.