HIPAA Compliance
Meaningful Use Risk Assessment Services
www.TrofiSecurity.com

Trofi Security's comprehensive HIPAA Risk Assessment Program was developed in direct response to the need for medical practices to have a security advocate to help them achieve **HIPAA Part 15** of the required **Meaningful Use Core Objectives and Measures.**

The Meaningful Use Risk Assessment Process must be conducted at least once prior to the beginning of each electronic health record (EHR) reporting period. While it is not impossible for a medical practice to conduct their own Risk Assessment, it is not always feasible or recommended, and should not be taken lightly. Most medical practices simply do not have the time, expertise and resources available to conduct a comprehensive assessment. By leveraging our expertise, you will have more time to focus on your patients, while Trofi Security ensures your practice's compliance through an evaluation of the following security control areas, as defined by the HIPAA Security Rule:

ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards are a special subset of the HIPAA Security Rule that focus on internal organization, policies, procedures, and maintenance of security measures that protect patient health information.

PHYSICAL SAFEGUARDS

The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

TECHNICAL SAFEGUARDS

The technology, and the policies and procedures for its use, that protect electronic health information and its access. This is typically firewalls, intrusion prevention, antivirus, and other technologies.

Our consultants will work with your team to address these control areas by performing the following key steps during the assessment and, optionally, beyond the assessment:

DURING THE ASSESSMENT:

- Identify the scope of the assessment
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of threat occurrence
- Determine overall level of risk
- Identify security measures and finalize assessment documentation

BEYOND THE ASSESSMENT: *(OPTIONAL)*

- Develop and Implement a risk management plan
- Implement security measures
- Evaluate and maintain security measures

To learn more about how we can help you through this process, **contact Trofi Security today.**

TROFI SECURITY®
INTELLIGENT INFORMATION SECURITY

844 GO TROFI (844 468 7634) | info@trofisecurity.com | @trofisecurity