**MEMORANDUM – 2 MINUTE BRIEFING 6**

**TO:** CASEY G. CEGIELSKI, PH. D, CISSP, CISA, CRISC

**FROM:** CENSORED

**DATE:** 10/23/19

The most important controls to focus on when implementing these systems will be the technical controls. Implementing the controls from each of the following categories (to the best of your abilities) will ensure that you are HIPAA compliant and threats to the EMR system are minimized. I will go over the important controls from each category in the next three paragraphs, as implementing them will provide confidentiality, integrity, and availability for your system.

Some technical controls that will be necessary to implement the EMR system are login identifiers, session timeouts, encryption (the most important), firewalls/routers, system logs and audit trails, data range and reasonableness checks, and a Public Key Infrastructure (PKI). These can be further sub-grouped into preventative, detective, and corrective categories of controls. The preventative technical controls are login identifiers, the Public Key Infrastructure (PKI), encryption, session timeouts, and firewalls/routers. The detective technical controls are the system logs and audit trails and the data range and reasonableness checks. The only control that could fall under the category of corrective technical would be the session timeouts.

Some physical controls that will be necessary wherever the EMR systems are implemented are locked doors, guards, CCTV cameras, fire detection/suppression systems, water detection systems, temperature and humidity detection systems (HVAC systems), electrical grounding and circuit breakers. These can be further sub-grouped into preventative, detective, and corrective categories of controls. The preventative physical controls are the electrical grounding, doors, guards, and the CCTV cameras. The detective physical controls are the CCTV cameras, and the corrective physical controls are the detection/suppression systems and circuit breakers.

Some administrative controls that will always be necessary when using the EMR systems are security plans (in case of emergencies), policies, procedures, hardening, patching, IDS, data backups, software testing, behavior rules, awareness training, and data loss prevention programs. These can be once again sub-grouped into preventative, detective, and corrective categories of controls. The preventative administrative controls are hardening, patching, data loss prevention programs, policies, procedures, behavior rules, awareness training and software testing. The detective administrative control is the IDS, and the corrective administrative controls are the data backups and security plans.