Technical Release Bulletin: RANSONWARE PREVENTION AND PROTECTION
For All SQA-V and SQA-VISION Systems
Issue Date: June 1, 2017

Background:

Ransomware is a form of malware that prevents or limits the use of a computer system until a sum of money has been paid. Variants, namely "WannaCry" (or similar) were observed infecting computers belonging to individuals and businesses, which included healthcare facilities and hospitals worldwide.

Recommendations:

1. All SQA-V and SQA-VISION systems are designed to operate "Offline", which means they do not connect to a network or the internet.
2. It is not recommended to use the SQA-V or SQA-VISION to run any other software, other than what is pre-installed by Medical Electronic Systems.
3. USB hard drives and flash drives not supplied directly by Medical Electronic Systems must be scanned for viruses or malware before being used to transfer data to and from the system.
4. Operating system patches and service packs must be installed by trained IT staff members using offline methods to transfer data (flash drives, discs, etc.)
5. If your IT staff recommends an operating system upgrade on V-Sperm Computers, please verify with MES support that the new operating system version will be compatible with the instrument and MES software. **Note: SQA-VISION instruments must remain on Windows 8.1 for proper operation.**
6. Medical Electronic Systems does not provide licenses for Operating System upgrades. In the case of an Operating System upgrade to V-Sperm computers, IT staff must purchase, install and license the operating system directly. MES will assist in reloading all necessary software pertaining to the system.
7. New V-Sperm computers with supported Operating Systems are available for purchase directly through Medical Electronic Systems.

Effective Date: JUNE 1, 2017

Approved by: **Salvador Arella Jr.** Sr. Biomedical Engineer / **Beni Cohen** Director R&D