"Commercial Off-The-Shelf Software (COTS) Policy Statement"

Carestream Health, Inc. (CSH) is committed to providing our customers with products and services that meet the highest standards of quality, safety and security. Medical Device development and support in particular demands the highest of standards. Our commitment recognizes that factors exist beyond our control in some information technology environments that could allow medical devices to become infected with computer code and cause abnormal behavior in the clinical application. Unwelcome malicious software is commonly referred to as viruses, logic bombs, trap doors, worms, or Trojan horses all of which, for simplification, are referred to below as malware. The purpose of this Policy is to describe the commitment CSH makes to insure its products and services operate properly when installed, and after the completion of any repairs or upgrades CSH may perform.

1. The CSH product warranty provides that all software in all of its products and services is free of malware at the time of installation or delivery.

2. CSH uses commercially reasonable efforts to ensure that all software in all computers or service tools used during the performance of repair services on customer equipment is free of malware before the service is rendered, and in the unlikely event that malware is introduced to a customer's system by a CSH computer or service tool, will promptly remove or quarantine any malware introduced by CSH at CSH's expense.

3. CSH will consider industry-standard best practices for hardening medical device operating systems through a range of techniques such as disabling unqualified remote management and access tools; securing access to storage devices and peripheral ports; securing built-in accounts; configuring login and password policies; securing file system access control lists; configuring data isolation and segmentation; securing protocols, interfaces and ports; configuring necessary network services; implementing an effective anti-virus program; implementing effective patch-management; securing administrative domain trust relationships; implementing file-system integrity monitoring; and/or implementing an intrusion detection/prevention system such as firewalls or Day Zero protection technologies.

4. CSH product specifications do not authorize customers to run anti-virus programs on CSH supplied medical devices due to concerns regarding clinical effectiveness and performance. CSH's product warranty and service terms exclude coverage related to problems caused by customer's installation or operation of such anti-virus programs. Customers should provide a Defense In-Depth environment that considers use of firewalls, intrusion detection, departmental isolation, switched networks and anti-virus technology operating on computing platforms that are not FDA regulated medical devices. System and internet access should be restricted to approved and trained users operating on approved systems and protocols.

5. CSH's product warranty and service terms provide that CSH is not responsible for the performance of its medical devices if customers make unauthorized software changes such as installing non-supported Off-the-Shelf (OTS) software, operating system and/or database security updates, alteration of operating system configurations or when malware infects CSH products during normal operation.

6. CSH may deploy OTS as software components with CSH medical devices. CSH will follow FDA guidelines and other relevant industry standards while providing qualified security updates to these OTS components based on availability from the OTS supplier. CSH will make reasonable efforts to inform customers of the availability of security updates or malware protection software it provides with its medical devices products, some of which may be offered as priced options on either an application update or upgrade basis. Termination of security updates from OTS suppliers will result in CSH's inability to provide security updates to the associated products.

7. CSH does not authorize, recommend or support any customer installed OTS, including anti-virus applications and custom developed software, on CSH medical devices. CSH may, when requested, provide information to customers

regarding mitigation of the adverse consequences of using unauthorized software, but CSH provides no warranties or representations regarding the quality of the information it provides for unauthorized OTS software, and all consequences of using OTS software are solely at customer's own risk.

8. Upon customer's request and at customer's expense, CSH offers remediation services under its services agreement to attempt to eliminate any product issues related to a customer's efforts to load non-supported OTS, custom software or any malware infections not caused by CSH in CSH-serviced equipment.

CSH is committed to offering malware-free products and services. Our goal is to be a repair and service resource for our customers if they discover their equipment has become malware-infected.