From: Rob Hill, Senior Vice President R&D and Chief Product Officer

Date: May 22, 2017

Re: WannaCry Malware Ransomware Attack

As stated in our letter (MKT/ARA/0517/0157) last week, Accuray has been continuing to work to minimize the potential for infection from the WannaCry malware and enhance cybersecurity for Accuray treatment systems and workstations. At the time of this letter, no Accuray systems or workstations have been reported to be infected by this malware.

Since the Accuray system firewall can reduce risk of infection by preventing the known transmission mode of this malware, we recommend that customers consider moving any Accuray system that is outside of the firewall to within the firewall. If you decide to pursue this option, Accuray will provide support in configuring the network to move those workstations within the firewall.

In the meantime, Accuray is in the process of testing its products with the Microsoft Security patches related to this vulnerability (see Microsoft Security Bulletin MS17-010). Starting Tuesday, May 30, Accuray will deploy the validated patches for the most vulnerable workstations that can reside outside the firewall. Those high risk systems include the Delivery Analysis workstation, MultiPlan, Accuray Precision, MD Suite workstations and CDMS Administration workstations. On May 30, Accuray will provide an update regarding further cybersecurity steps that we are taking.

In the event any Accuray workstation becomes infected, immediately disconnect the system from the network by removing the Ethernet cable from the computer system or, alternatively, turning the computer off and contacting Accuray Service.

If you have any questions or concerns, please contact Accuray's Service team.