BRiCare™

Security and Privacy Statement

Ensuring the security and privacy of your data is of the utmost importance. The BRiCare™ application uses numerous measures to ensure the highest level of security and privacy.

This statement is intended to provide you with a summary of the security measures implemented in BRiCare™ and our security and privacy policy. This statement provides information of the security layers that are implemented in BRiCare™.

BRiCare™ utilizes some of the most advanced technology for Internet security available today. We use industry-standard HTTPS (SSL) VPN security technologies to protect data transfer. The VeriSign Extended Validation Certificate (RSA 2048 bit) is used to ensure complete authentication, verifies Bio-Rad Laboratories as the authorized owner of the website and provides daily malware scans of the site. In addition, BRiCare™ is hosted in a secure server environment that uses firewall, anti-virus and other advanced technologies to prevent interference or access from outside intruders.

The BRiCare™ applet was developed based on the Secure Development Life Cycle (SDLC) methodology. Data transmissions from the applet to the server are initiated only by the applet (outbound only) and highly encrypted using VeriSign SSL (port 443). No personally identifiable information (PII) is sent. Once the data is transmitted to the BRiCare™ secure server it is deleted from the applet computer.

The minimal footprint applet is designed not to interfere with the computer operation.

Remote sessions are initiated by Bio-Rad authorized personnel and all sessions must be approved by the customer. Remote sessions are visible in real time to the customer and can be terminated at any time. All remote sessions are highly encrypted (AES 256bit), authenticated and fully audited. All file transfers use encryption and SSL technology to ensure the integrity of the data. A detailed audit log is available for each remote session, on the customer‘s computer.

Bio-Rad is committed to respect confidentiality of customer‘s and patient‘s data and never disclose or forward such information.

BRiCare™ undergoes frequent security related inspections and risk assessment by a leading security company. BRiCare™ and its underlying infrastructures and components have been successfully designed and tested to meet the requirements of the CLSI standard for „Remote access to Clinical Laboratory Diagnostic Devices via the Internet“. These requirements are also appropriate to ensure security for devices used in other applications.

BIO-RAD

EU-IM-2-02/13E