CYBERSECURITY ASSURANCE PROGRAM CERTIFICATE

Certificate
ULCAP_1009

Issue date
2024-06-26

Expiration date
2025-06-26

Test Report Number
4791266251-001

This is to acknowledge that

Becton Dickinson Life Sciences

155 North McCarthy Boulevard
Milpitas, CA, 95035, US

has had

FACSuite Clinical Software

FACSuite Clinical v1.6.0.3080 US-RUO
Software Version: 1.6.0.3080 US-RUO

evaluated and meets the requirements of the standard

UL 2900-2-1: 2023A

Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems, First Edition September 1, 2017 including revisions through September 21, 2023.

Program owner:
Dean Zwarts

Dean Zwarts, Senior Business Manager

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL Solutions does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the Service Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL Solutions trademarks on the Certified Product. UL Solutions trademarks may only be used if the Certified Product is also covered under the applicable UL Solutions mark program(s).

Conditions of Certificate

The following conditions must be met for the product to continue to be in compliance with this certificate:

1. FACSuite must be configured in accordance with the BD application and configuration manuals to maintain cybersecurity best practices.
2. FACSuite as well as network connections are to be under physical access control and hard wire connected.
3. FACSuite must be regularly updated per BD’s recommendations, for the latest security patches of the OS and 3rd party libraries.