Cybersecurity in healthcare

Protecting patient data integrity, accessibility and privacy

Cybersecurity is a key healthcare concern with substantial financial burdens.

Globally, the average cost of a data breach in the healthcare industry is $6.45M.[1]

Laboratory instruments that are connected to information systems, are at increased risk of cyberattack, putting protected health information (PHI) and patient safety at risk.

Cyberattacks may also impact an institution's reputation, disrupting patient care and causing loss of productivity.

To protect patient safety, healthcare organizations should choose an informatics solutions designed with a robust cybersecurity framework.

BD

BD Synapsys™ informatics for blood culture is designed to support the secure analysis and communication of blood culture results and patient information.

BD Synapsys™ informatics meets UL CAP cybersecurity standards, is SOC 2 compliant, and provides:

- Patient confidentiality and blood culture data integrity through strong data encryption
- Audit logging to track usage of the BD Synapsys informatics
- Role-based access control, through authentication with Active Directory integration
- Protection against evolving cybersecurity threats with up-to-date technology and continuous cybersecurity support including advanced AI-based anti-malware and routine security patching

The UL Cybersecurity Assurance Program (UL CAP)[2] is an **independent third-party testing and certification program** for network-connectable products and software components such as medical devices.

UL CAP certification **verifies compliance** with UL 2900, a series of standards validating that a product offers a reasonable level of **protection against cybersecurity risks** that may result in unintended or unauthorized access, change or disruption.

The US government recognizes UL CAP in the Cybersecurity National Action Plan as a key initiative in the coordinated effort between the **Department of Homeland Security (DHS)** and the private sector.

Developed by the American Institute of CPAs (AICPA), SOC 2[3] defines criteria for managing customer data based on five "Trust Services Criteria": security, availability, processing integrity, confidentiality and privacy.

SOC 2 is an auditing procedure that **allows service providers to securely manage data to protect the interests of organizations and patient privacy.**

For security-conscious institutions, SOC 2 compliance is an **increasingly important requirement** when considering informatics providers.

Additional reasons to trust in the BD Synapsys informatics solution:

- Includes recognized standards in its product design and security framework (i.e., NIST, ISO, DISA STIG, CWE/SANS)
- Incorporates the CylancePROTECT® AI-based, second generation anti-malware solution
- Has undergone extensive penetration testing (i.e., authorized simulated cyberattacks to evaluate the security of the system):
  1. Rigorous internal testing by the BD "red team"
  2. US FDA-supported DEFCON 2019 Biohacking Village participation

The BD BACTEC™ system, powered by BD Synapsys™ informatics, delivers blood culture results while protecting patient data integrity, accessibility and privacy.

1. Cost of a Data Breach Report 2019 by Ponemon Institute & IBM Security
2. https://www.synopsys.com/blogs/software-security/synopsys-and-ul-announce-ul-cybersecurity-assurance-program/
3. https://www.imperva.com/learn/data-security/soc-2-compliance/

BD Life Sciences, 7 Loveton Circle, Sparks, MD 21152-0999 USA
Tel: 1.800.638.8663

bd.com

393-WW-0320. June 2020