CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Cybersecurity Requirements in Clinical Laboratories

November 7, 2024

Disclaimer

- This presentation was prepared for informational purposes and is not intended to grant rights or impose obligations. Every reasonable effort has been made to assure the accuracy of the information within these pages.

- This publication is a general summary that explains certain aspects of the Clinical Laboratory Improvement Amendments (CLIA) Program, but is not a legal document. The official CLIA Program provisions are contained in the relevant laws, regulations, and rulings. Links to the source documents have been provided within the document for your reference.

- The Centers for Medicare & Medicaid Services (CMS) employees, agents, and staff make no representation, warranty, or guarantee that this compilation of CLIA information is error-free and will bear no responsibility or liability for the results or consequences of the use of this guide.

Cybersecurity Requirements in Clinical Laboratories

Scope of the issue:[1]

- Ransomware attacks accounted for 70% of the successful cyberattacks on healthcare organizations
- 1,613 global healthcare organizations suffered an attack in the first 3 quarters of 2023
- Cyberattacks cost an average on $11 million per breach

State of the Industry: [2]

- More than one in four ransomware attacks affects patient care
- Approximately half of the healthcare organizations attacked said patient data was compromised
- More than one third of healthcare companies report not having a cybersecurity response plan

[1] https://www.healthcarefinancenews.com/news/healthcare-cyberattacks-are-costing-average-11-million-breach

[2] https://www.healthcaredive.com/news/healthcare-ransomware-cyberattack-impacts-patient-care-software-advice/716971/

Cybersecurity Requirements in Clinical Laboratories

Current CLIA cybersecurity regulatory requirements:

42 CFR 493.1251(b)(14)

The procedure manual must include the following when applicable to the test procedure:

- Description of the course of action to take if a test system becomes inoperable
  - Accompanying Interpretive Guidance: “*Laboratory information systems (LIS) procedures must be available to operators. Instructions should identify the individual(s), either by name or position, to notify if the LIS goes down or if a system error occurs.*”

Cybersecurity Requirements in Clinical Laboratories

Current CLIA cybersecurity regulatory requirements:

42 CFR 493.1291 Standard: Test report. The laboratory must have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific data are accurately and reliably sent from the point of data entry (whether interfaced or entered manually) to final report destination, in a timely manner…

- Accompanying Interpretive Guidance: “If the laboratory uses a LIS or facsimile, what security measures have been instituted to ensure that transmitted reports go directly from the device sending reports to the authorized person, their personal representative (if applicable), and others who are identified as responsible for using the test results on the requisition? .”

Cybersecurity Requirements in Clinical Laboratories

Current CLIA cybersecurity regulatory requirements:
42 CFR 493.1254(a)(1) *Maintenance as defined by the manufacturer and with at least the frequency specified by the manufacturer.*

- The Interpretive Guidelines define "as defined by the manufacturer" to include each piece of equipment/instrument it uses, including those that are peripherally involved in patient testing. The guidance also explicitly states: *The laboratory must perform and document maintenance as specified by the manufacturer for the LIS computer and devices such as monitors, printers and modems. All devices must be maintained to ensure accurate, clear, and interference-free transmission.*
- The Interpretive Guidance offers specific probes to surveyors to help assess LIS functionality and cybersecurity: *Are LIS system components (e.g., server, hard drives, disk packs) maintained according to the manufacturer's instructions? When downtime is required to perform maintenance on LIS equipment, how are LIS users notified?*

Cybersecurity Requirements in Clinical Laboratories

- Recommendations from the NCC (National Computing Centre) Group as reflected in the January 16, 2024, edition of the Dark Report:
  - Employ multifactor authentication on all external facing internet connections
  - Segregate legacy operating systems from the network
  - Back up files in multiple offline locations
  - Create patches to address vulnerabilities frequently
  - Train staff is awareness of security threats
  - Draft and rehearse incident management plans

Cybersecurity Requirements in Clinical Laboratories

The questions for CLIAC on this topic:

Would CLIAC recommend stronger regulatory requirements related to cybersecurity protocols for the laboratory setting?

- What is the real-world risk of maintaining the status quo?
  - Weighing the likelihood of a cyberattack on a given laboratory
  - Assessing the current existing incentives to preventing an attack
- What is the cost of regulations that require the steps on the previous slide?
- What are the benefits of such regulations?
- How much time would a laboratory need to make such changes?

- Any alternative recommendations from CLIAC (Study group, RFI, etc.)