No Network? No Problem. Preparing for a Cyberattack in the Clinical Laboratory

Monica Coyle, MHA, Tim Faber, MA, Becky Hinchley, MA, John Osborn, MSc

BACKGROUND: Between January 1, 2011, to December 31, 2021, there were 3,822 breaches of Protected Health Information (PHI) in the United States which affected 283,335,803 people[1]. Of those, 41.7% were hacking or Information Technology related, and 74% involved health care providers. In a national survey, while 82.4% of hospitals included cybersecurity disasters in their Hazard Vulnerability Analyses (HVAs), over half did not have an Emergency Operations Plan in place related to cybersecurity[2].

OBJECTIVES: In alignment with continual readiness for emergency preparedness, Mayo Clinic requires its business units to develop response plans for a cyberattack. These response plans should guide continued delivery of life-saving and life-sustaining care and inform prioritization while full network function is restored. Laboratory services are essential to continued safe patient care during a cyberattack, and effective continuity plans are required to support clinical operations if one were to occur.

PLANNING & IMPLEMENTATION METHODS: During the pandemic, every work unit established a continuity plan defining what services would be prioritized as staffing became constrained. These plans provide a guide for an orderly transition from conventional to contingency standards of care with triggers for modifying or reducing services and activities[3]. In the clinical laboratories, the order in which testing would be discontinued is defined and reviewed yearly as part of emergency preparedness planning. In a ransomware event, access to the intranet and internet will be immediately suspended, as will access to the Electronic Health Record (EHR) and the Laboratory Information System (LIS). Ordering, resulting, and intermediate workflows will need to be performed manually and on paper. Laboratories with immediate patient care functions, such as the hospital lab, blood bank, and toxicology lab, were prioritized for initial planning efforts.

To inform continuity plans, lab managers were asked the following for each instrument in their lab:

- Can it be manually operated and generate valid results without a network connection?
- Can results be printed? If not, can results be viewed on the instrument?
- Is there an existing manual back-up results form?

Platforms that are network-dependent were identified and the tests performed on those instruments flagged The remaining tests that can be performed were matched to the clinical priority established in the pandemic plan. Lab managers assessed the staff required to perform each test in an entirely manual manner. The testing that could be performed with typically scheduled staff on duty was defined. The test catalog was grouped into the following lists, and resource needs identified tests and tasks that:

- Would require additional specially trained laboratory staff
- Would require additional laboratory staff
- Could be performed by non-laboratory staff

RESULTS & LESSONS LEARNED: Most laboratory instruments can run without network connectivity, but all required specimen information must be hand-entered and results manually reconciled and communicated back to ordering providers. Almost all lab testing procedures will require some modification, and lab throughput will be significantly decreased. The return to unfamiliar paper-based ordering and result communication will present significant patient safety risk through specimen or result misidentification. Staffing will need to be augmented by other trained lab professionals as well as non-lab personnel to handle the increased specimen and data management needs. Impairment of building control systems will impact air handling, air temperature, and potentially other essential utility services, which will further constrain lab operations. Collaborative planning with hospital leaders will need to occur to direct testing capacity to the highest priority patient care needs.

As part of emergency preparedness/continual readiness, Mayo Clinic has required a cyberattack plan for its business units. Through the process of planning a response for a cyberattack, there are key items that need to be considered in evaluating all operational needs associated with a response to a cyberattack - patient care continuity, a triage and prioritization process, identifying all networking interdependencies, and outlining communication pathways.

1. Chen, PH., Bodak, R. & Gandhi, N.S. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *J Digit Imaging* **34**, 731–740 (2021). https://doi.org/10.1007/s10278-021-00466-x

2. Tin D, Hata R, Granholm F, Ciottone RG, Staynings R, Ciottone GR. Cyberthreats: A primer for healthcare professionals. Am J Emerg Med. 2023 Jun;68:179-185. doi: 10.1016/j.ajem.2023.04.001. Epub 2023 Apr 5. PMID: 37061434.

3. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A National Survey of Hospital Cyber Attack Emergency Operation Preparedness. Disaster Med Public Health Prep. 2023 Mar 22;17:e363. doi: 10.1017/dmp.2022.283. PMID: 36945857.