Research Article

Clinicians' Perspectives on the Impact of a Ransomware Attack on a Chemical Pathology Laboratory at a Tertiary Hospital in South Africa

Ameerah Davids[1,2], Aaqilah Fataar[1,2*], Asande Zama[1,2], Zakeeya Kadwa[1,2], Craig J Andrews[1,2], Mikayla N Morris[1,2], Thumeka P Jalavu[1,2], Elsie C Kruger[1,2], Annalise E Zemlin[1,2]

[1]*Department of Pathology, Division of Chemical Pathology, Faculty of Medicine and Health Sciences, Stellenbosch University, Cape Town, South Africa*

[2]*Department of Pathology, Division of Chemical Pathology, National Health Laboratory Service, Tygerberg Hospital, Cape Town, South Africa*

Article Info

[*]***Corresponding Author:***
Aaqilah Fataar
Phone: +27 21 938 4643
E-mail: aaqilah.fataar@nhls.ac.za
Tygerberg Hospital, Francie van Zijl Drive, Parow, Cape Town, South Africa

Keywords

Ransomware, cyberattack, patient safety

Abstract

Objectives: This study aimed to explore clinicians' experiences during a ransomware attack at a public academic hospital in South Africa and assess the perceived impact of chemical pathology laboratory service disruptions on patient care.

Methods: A cross-sectional survey was conducted between September and December 2024. An electronic questionnaire was distributed to clinicians to gather data on their experiences during the ransomware attack, including impacts on patient care and workload. To assess changes in test requesting practices during this period, volume data for both critical (creatinine) and non-critical (vitamin B12) tests from routine annual laboratory reports were analysed.

Results: Among the 58 respondents, 84% reported increased stress levels, while 78% indicated delayed diagnoses during this period. Laboratory test volumes decreased during the attack period compared to previous years, with reductions of 26.8% for creatinine and 34.1% for vitamin B12 tests. Clinicians primarily struggled with result retrieval and reported substantial disruptions to patient care.

Conclusions: This study provides valuable insights into clinicians' perspectives on the impact of a laboratory ransomware attack. The findings highlight the critical need for investment in both cybersecurity infrastructure and comprehensive contingency planning to safeguard patient safety and minimise disruptions during future cyber incidents.

Key Points: This study addresses how ransomware attacks disrupt and impact clinician workflow in resource-limited hospital settings. Medical professionals should develop practical contingency plans for accessing and managing essential laboratory data during cybersecurity incidents to minimise care disruptions. The most significant finding was the dual impact of technical service disruption alongside pronounced clinician psychological stress, creating a compounded effect on healthcare delivery.

Introduction

Health Information Systems (HIS) are both crucial to modern healthcare delivery and increasingly vulnerable to cyber threats. These systems facilitate the easy storage, retrieval, and generation of high-quality information. Health information technology employs computer hardware and software to create these systems, which are essential for sharing healthcare data and supporting informed decision-making [1]. Given the sensitive nature of the data collected by HIS, cybersecurity is a critical consideration. Ensuring robust cybersecurity measures is essential for safe and effective health technology use and maintaining patient safety in the current digital era. Failing to implement adequate cybersecurity measures can leave an institution vulnerable to ransomware attacks. These attacks involve malicious software that renders electronic systems unusable until a ransom is paid, effectively holding the institution hostage [2]. The consequences of such attacks extend far beyond financial concerns.

Cyberattacks on healthcare are not only costly but negatively affect patient care. Additionally, laboratories and healthcare facilities are often unprepared and lack robust contingency protocols for prolonged downtime periods. Multiple authors have attempted to describe the effects of prolonged downtime on the laboratory and stakeholders, including patients [3, 4]. Patient care relies on laboratory data, with up to 70% of clinical decisions regarding diagnosis, treatment, or prevention being made based on this information [5]. Therefore, disruptions in laboratory services, such as those caused by a ransomware attack, can severely impact patient care and compromise patient safety. The National Health Laboratory Service (NHLS) in South Africa, the backbone of the nation's diagnostic infrastructure, delivers more than 80% of the country's pathology services [6]. On June 22, 2024, the NHLS suffered a ransomware attack, which resulted in the inability to utilise information technology (IT)-related systems, including the laboratory information system (LIS) (InterSystems TrakCare® Lab Enterprise, Cambridge, Massachusetts, United States). Consequently, many automated processes reverted to manual operations, while new and historic patient laboratory results were inaccessible. This change led to delays in the turnaround time for patient results and made it challenging for clinicians to access historic results and view new results timeously [7]. There is currently a critical paucity of evidence examining clinicians' perceptions on the impact of laboratory downtime due to ransomware attacks on patient care, particularly in resource-limited settings.

This study aimed to investigate clinicians' perspectives at Tygerberg Hospital (TBH), a public tertiary academic hospital in Cape Town, South Africa, regarding the ransomware attack and to evaluate the perceived consequences of chemical pathology laboratory service disruptions on clinical decision-making and patient management. The findings provide critical insights for developing effective contingency protocols in resource-constrained healthcare environments.

Methods

Ethical Considerations

The study was approved by the Human Research Ethics Committee of Stellenbosch University (N24/08/095) in September 2024. Respondents were provided with detailed information regarding the study purpose, procedures, and voluntary nature of participation before being included in the study, and their completion and submission of the survey was taken as implied consent. All data were collected anonymously to maintain confidentiality.

Study Design

This study used a cross-sectional survey design to evaluate the impact of the June 2024 laboratory ransomware attack on clinicians' workflows, stress levels, and perceptions of laboratory performance at TBH. The survey was distributed electronically across all clinical departments, targeting clinicians of all ranks and specialities who were actively engaged in patient care during the downtime period. Data were collected and managed using Research Electronic Data Capture (REDCap) electronic data capture tools hosted at Stellenbosch University. Access to the database required two-factor authentication and was restricted to study authors.

Study Setting and Population

This study was conducted at Tygerberg Hospital (TBH), a 1384-bed state-owned teaching hospital affiliated with Stellenbosch University. TBH provides healthcare services to approximately 3.6 million people, with its onsite NHLS facility processing an average of 125,000 chemical pathology tests monthly. As a public healthcare institution, TBH predominantly serves communities with limited resources in the Cape Town Metro East sub-districts while also receiving referrals from rural catchment areas throughout the Western Cape province.

The survey targeted clinicians across all levels of training (from medical interns to specialist consultants) employed at TBH who were directly responsible for patient management decisions during the June – July 2024 ransomware attack. This period saw significant disruption to the hospital's normally robust laboratory information systems and services.

Laboratory Response to Downtime

The ransomware attack on the laboratory IT systems necessitated rapid operational adjustments to maintain essential service delivery. A key measure involved prioritising critical tests while temporarily suspending specialised testing. The laboratory published a prioritised test list to guide clinicians and ensure efficient resource allocation during this period.

With electronic systems compromised, alternative result retrieval methods were implemented. Clinicians either contacted the laboratory directly or physically collected paper printouts from analysers. To improve accessibility, these physical result copies were systematically organised by patient ward location.

Three weeks into the incident, limited digital access was restored through Single Patient Viewer (SPV), an alternative electronic platform maintained by the Western Cape Department of Health (DoH). This web-based portal, which functions as an integrated electronic health record system and retains historical data, became a crucial interim solution. Through collaboration between the NHLS and the DoH, select laboratory results were systematically uploaded to SPV, partially restoring clinicians' ability to access patient results electronically.

However, significant limitations persisted. Manual and semi-automated chemistry test result were not integrated into the SPV platform, and technical issues occasionally prevented successful result uploads, creating gaps in the available electronic data that continued to challenge clinical decision-making.

Data Collection Methods

The survey (Supplementary Table 1) was collaboratively developed to evaluate key aspects of clinicians' downtime experience following a ransomware attack affecting the NHLS. The survey collected demographic information, including years of clinical experience and primary clinical setting of the respondents. Participants provided feedback on the impact of the downtime on patient care, including delays in diagnosis, treatment decisions, investigations, patient referrals, surgical scheduling, and hospital discharge. The survey also assessed effects on clinicians themselves, such as increased workload and stress levels. Additionally, respondents evaluated the laboratory's preparedness, communication effectiveness, and result accessibility during the downtime. A five-point Likert scale was used for closed-ended questions, while open-ended questions allowed for additional feedback and recommendations.

Survey development followed a rigorous process. Initial drafts were refined through team discussions. To ensure clarity, the survey underwent pre-testing among laboratory staff to assess question coherence, platform usability, and branching logic. Feedback was used to refine wording, structure, and resolve technical issues. Pre-testing responses were excluded from the final dataset.

Distribution employed a multi-faceted approach to maximise clinician engagement. Following ethics approval, the electronic survey was distributed until 31 December 2024, with fortnightly reminders to enhance response rates. Quick response (QR) codes linking directly to the survey were included on posters placed in hospital wards and outpatient departments. Additional reminders included direct messages to team representatives and authors physically visiting clinical areas. Despite these comprehensive efforts, it remained challenging to determine precisely how many clinicians encountered or interacted with the survey.

To complement survey findings, routine laboratory statistics were analysed to provide insights into test volume reductions during the downtime period. Creatinine and vitamin B12 were purposively selected as sentinel analytes to represent contrasting clinical priorities: creatinine as a high-volume, clinically critical test included on the laboratory's prioritised test list, and vitamin B12 as a non-urgent, non-priority test. Numbers for both tests were compared for the month of July across years 2021 to 2023 to account for seasonal variation and establish a pre-attack baseline against which the ransomware period (July 2024) could be interpreted.

Statistical Analysis

Data collected from the survey were analysed using both descriptive and inferential statistical methods to explore the impact of laboratory downtime on clinicians. Categorical variables, including demographics and responses to Likert-scale questions, were summarised as frequencies and percentages. Likert-scale data were further analysed to calculate agreement levels for key metrics, such as stress levels, diagnostic delays, and perceptions of laboratory performance. Survey data were accessed from REDCap, then underwent systematic extraction, cleaning, and analysis. Routine testing volume data for July across four consecutive years (2021, 2022, 2023, and 2024) were compared using analysis of variance (ANOVA) to assess significant differences between years. All statistical analyses were conducted using R version 4.3.1, with specific analytical and visualisation functions from the dplyr, ggpubr, and ggplot2 packages.

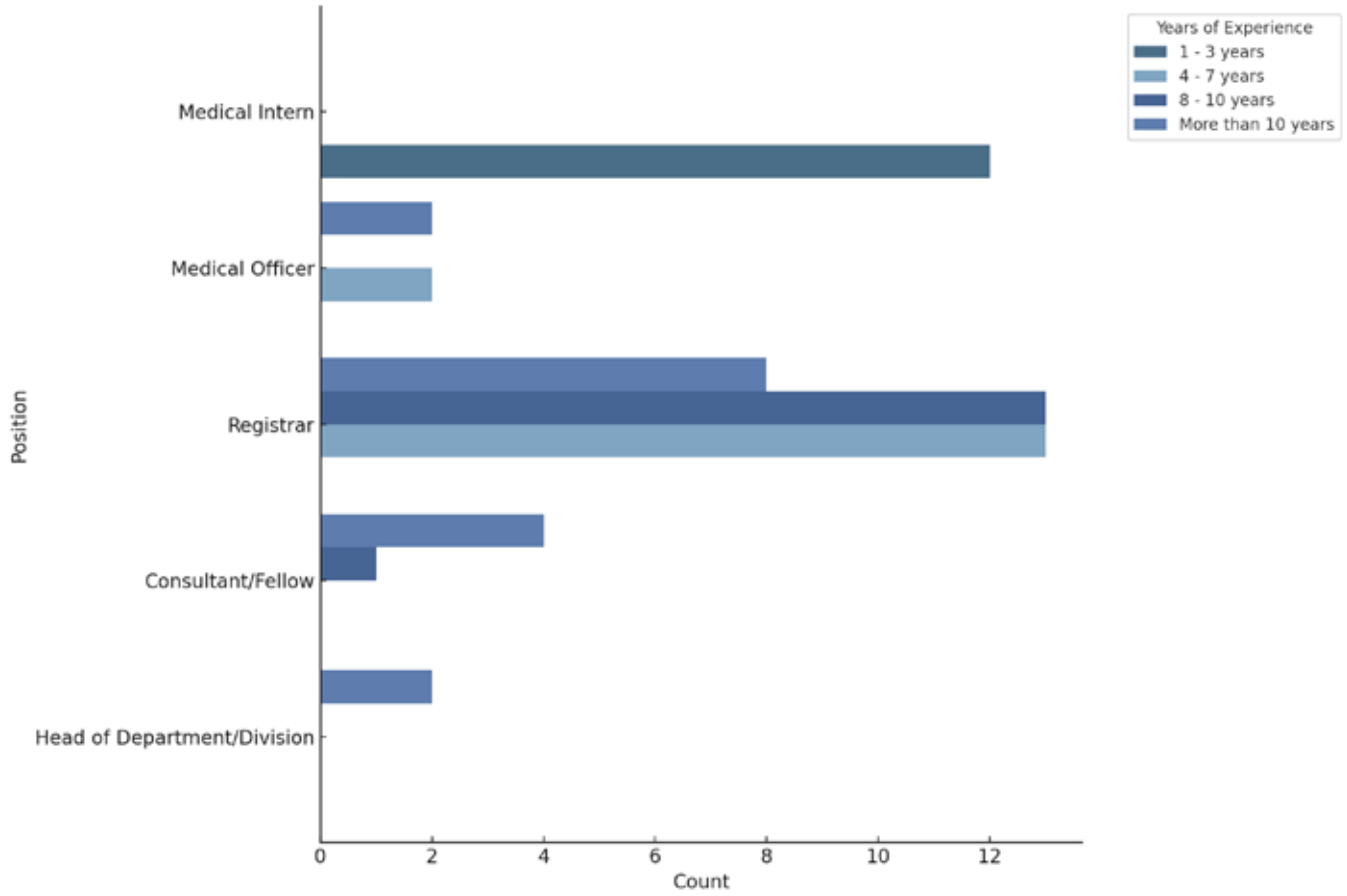
Results

A total of 63 responses were received, of which 58 were complete and included in the analysis. Five responses (7.94%) were excluded: one from a clinician who did not work at TBH and four because they were incomplete.

Demographics

Figure 1 depicts the demographics of the study respondents. Of the 58 clinicians who responded, most were registrars (59%, n=34), with a smaller representation of consultants and fellows (9%, n=5). Most participants reported having extensive clinical experience, with 28% (n=16) indicating more than 10 years, 24% (n=14) reporting 8–10 years, and 26% (n=15) reporting 4–7 years. The clinical settings of the respondents varied, with the majority working in inpatient care (40%, n=23) or a combination of in- and outpatient care (59%, n=34).

Figure 1: Distribution of years of experience among the 58 healthcare professional respondents by rank at Tygerberg Hospital, September 2024 to December 2024.



Summary of Laboratory Response to Downtime

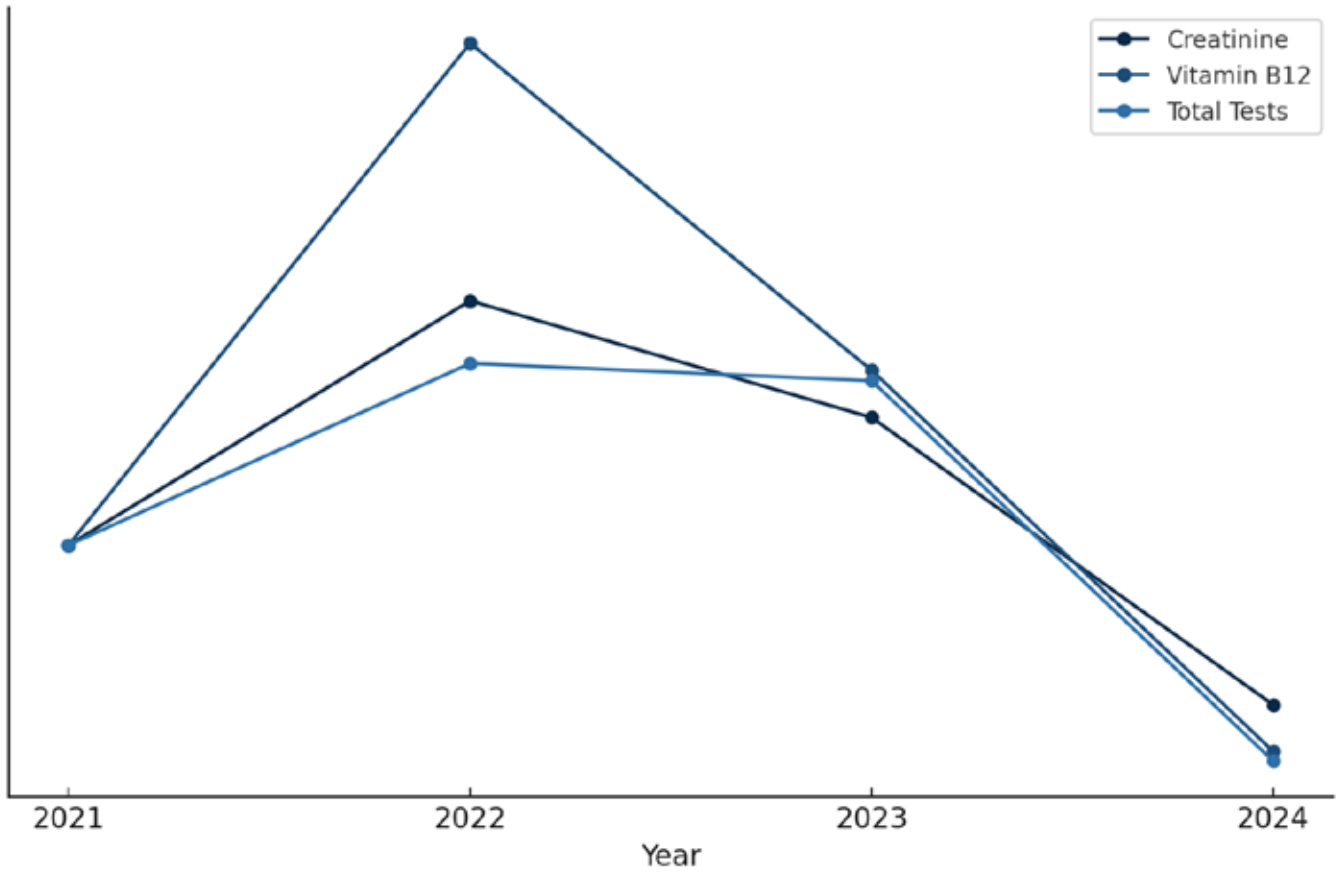
Clinicians acknowledged the efforts of the Chemical Pathology laboratory staff during the downtime, with 74% (n=43) agreeing that the staff were helpful and made efforts to assist clinicians. Moreover, 67% (n=39) of respondents believed the laboratory attempted to reduce delays in turnaround times, demonstrating a proactive approach to managing the situation. While 52% (n=30) agreed that communication of critical results was timely, 48% (n=28) reported issues with missing results, and 39% (n=23) noted difficulties interpreting results due to the lack of reference intervals, automatic calculations, or interpretive comments. Additionally, only 43% (n=25) of respondents felt the laboratory was adequately prepared for the unexpected downtime.

Clinicians' Use of the Critical Test List

While the majority (68.97%, n=40) reported scaling down testing using the published critical test list, 22.41% (n=13) indicated they were unaware of its availability, and 8.62% (n=5) reported not scaling down testing at all.

Test volumes for creatinine, a test included on the critical test list, showed a 26.8% reduction in July 2024 compared to previous years, while vitamin B12, a test not on the priority list, experienced a sharper decline at 34.1% (Figure 2). Total test volumes dropped by 34.3% overall.

Figure 2: Normalised test volumes for creatinine, vitamin B12, and total laboratory tests at Tygerberg Hospital during July months from 2021 – 2024, including the ransomware attack period of July 2024.



Clinician Response to Alternative Result Retrieval Methods

Collecting physical copies of results directly from the laboratory emerged as the most frequently used method, reported by 55% (n=32) of respondents. Additionally, 22% (n=13) relied on calling the laboratory for urgent results. Many clinicians noted that the ward-specific result filing system implemented during the downtime was inefficient, with 47% (n=27) disagreeing or strongly disagreeing that it facilitated timely access to results. On the other hand, direct communication with laboratory staff was highlighted as a helpful approach, with 71% (n=41) agreeing that laboratory personnel made efforts to assist during the downtime.

Operational Challenges

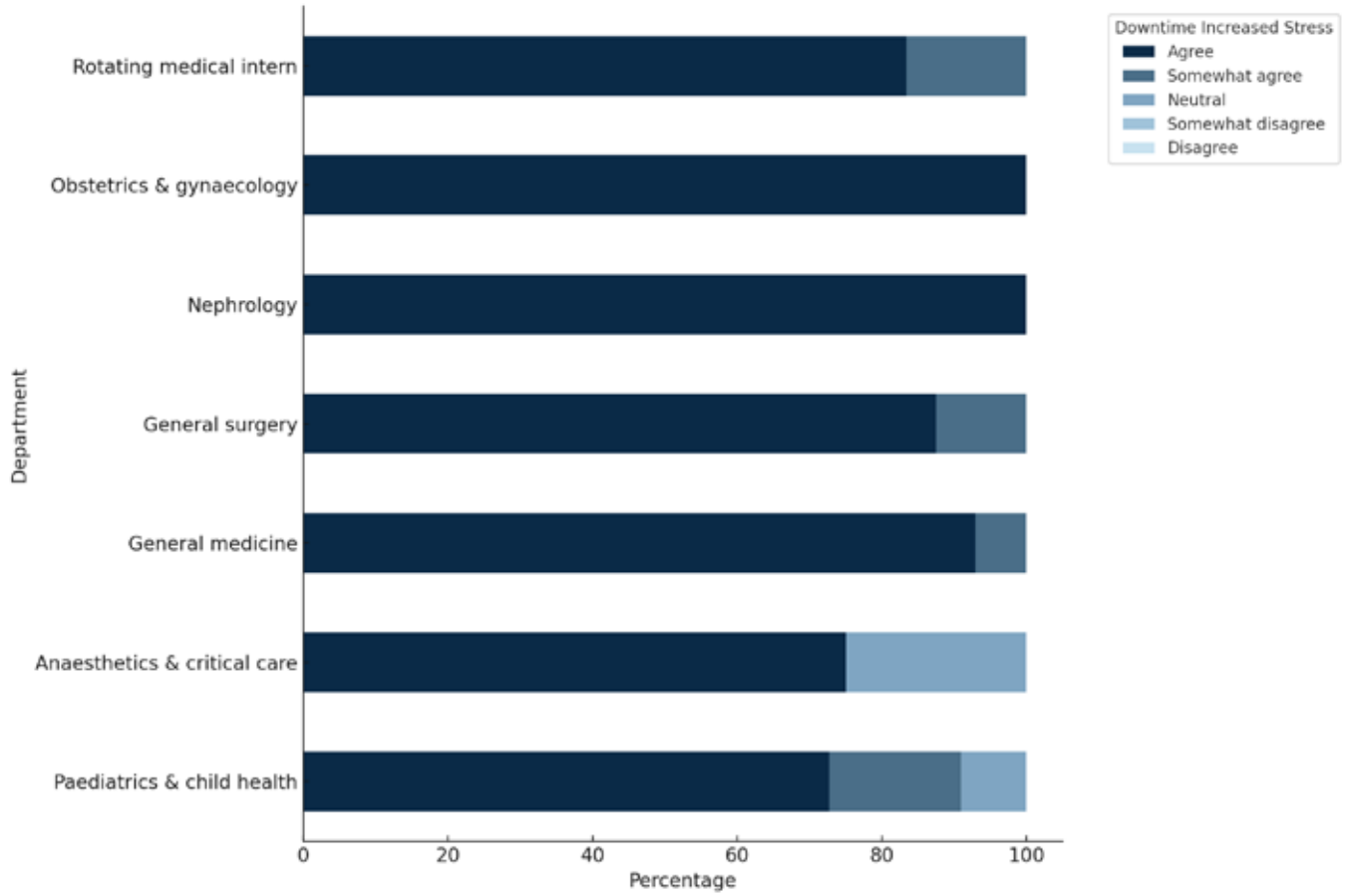
Delays in obtaining laboratory results were widely reported, affecting diagnostic timelines (78% agreed, n=45) and decisions regarding initiating or discontinuing patient treatment (73%, n=42). The nephrology department reported the highest percentage of delayed diagnoses (100% agreed), with general surgery and medical interns reporting similarly high levels (87.5% and 83.3% agreed, respectively).

Furthermore, 69% (n=40) of respondents indicated that the downtime impacted the scheduling and availability of special investigations, such as computed tomography scans, and 65% (n=38) reported delays in interdepartmental patient referrals. Surgical schedules were also disrupted, with 62% (n=36) noting delays in emergency surgery scheduling and 58% (n=34) reporting challenges with elective surgeries. Clinicians from Anaesthetics and Critical Care reported the highest rate of delays in emergency surgeries (100% agreed). Prolonged patient discharge and increased length of stay were significant issues for 60% (n=35) of respondents, reflecting the ripple effect of delayed laboratory results on hospital efficiency. The unavailability of specialised testing during downtime further complicated patient management for 68% (n=39) of clinicians.

Impact on Clinician Wellbeing

Most respondents (84%, n=49) reported that the downtime increased their stress levels, with 42% (n=24) strongly agreeing. Additionally, 71% (n=41) indicated that the downtime led to extended working hours. Stress levels were highest among the nephrology and obstetrics and gynaecology teams (100%), followed by general medicine (92%) and general surgery (87.5%) (Figure 3). Notably, none of the respondents disagreed with the statement that the downtime increased their stress levels.

Figure 3: Distribution of stress-related responses among healthcare professionals by department at Tygerberg Hospital, September 2024 to December 2024. Responses are presented as percentages on a five-point Likert scale.



Discussion

The study findings highlight the significant impact of the ransomware-induced downtime on clinical workflows, laboratory services, and clinician well-being. While the majority of clinicians acknowledged the efforts of the chemical pathology laboratory staff, many reported challenges with communication, missing results, and difficulties interpreting laboratory results.

In the chemical pathology laboratory, analyser-printed results were made available to clinicians once laboratory staff authorised them. However, these results lacked interpretive comments, reference intervals, and automated calculations. The impact of this was seen in the 39% (n=23) of respondents who noted challenges in report interpretation. This could have influenced the perception of more than half of the respondents (57%, n=33), who perceived the laboratory as unprepared for the unexpected downtime. In 2021, Duffy et al. described producing paper-based reports during downtime in Ireland following a cyberattack on their information technology infrastructure, where they similarly lost access to laboratory systems. They described a high level of scientific input and manual processes required for these reports [8]. Given our already resource-limited setting, these reports were not developed and would likely have increased the burden on laboratory staff [7]. As noted, the analyser-printed reports provided to clinicians lacked reference intervals. To address this, we provided reference intervals to hospital management for staff dissemination. However, it is unclear if the documentation was distributed to all clinicians, given the difficulty experienced by some respondents. This highlights the importance of establishing clear protocols with input from clinicians and management to ensure effective communication and dissemination of information between laboratory and clinical staff.

The European Federation of Clinical Chemistry and Laboratory Medicine (EFLM) Task Force Preparation of Labs for Emergencies recommends the use of telephonic communication for critical laboratory results during downtime; however, they reported that there is still uncertainty regarding the preferred method of delivery of other test results [9]. Clinicians found direct communication with laboratory staff to be the most helpful approach to obtaining laboratory results compared to the other available methods described. Nearly half of the respondents found the box sorting system unhelpful, likely due to incomplete or illegible laboratory request forms that impeded accurate result sorting. As described by Cassim and Chapanduka, the distribution of results took the longest time during the NHLS ransomware attack; this likely greatly

impacted service delivery, especially before the introduction of SPV[7].

Stowman et al. described the reporting practices for anatomical pathology results during a systemwide cyberattack in the United States in 2020, which disrupted their LIS. They adopted a manual process where reports were typed by support staff, hand-signed by pathologists, and faxed to clients. They noted barriers to using fax included the lack of provider contact details or illegible information on laboratory request forms, an aspect also experienced by our laboratory staff when attempting to disseminate results. Additionally, digital faxes were rendered unusable, and only analogue faxes worked [10]. They further noted the challenges of managing phone calls about missing specimens or reports, which mirrored our laboratory's experience during the ransomware attack. This shows that even in centres with enhanced infrastructure for result dissemination, the distribution of results remains challenging in the absence of an LIS. Given the limited resources available during downtime, it was challenging to effectively distribute results telephonically. Goodwin et al. reported on a cyberattack which occurred in the United States in October 2020. They noted that results were also distributed by hospital runners who collected hard copies from a designated passage while delivering patient specimens to the laboratory [4]. Similarly, we implemented a practice where hard copies were placed in boxes organised by test request location for collection. Inefficiencies in this system may arise from missing ward location information or discrepancies between a patient's current admission location and their initial contact point, such as the emergency department, labour ward, outpatient clinic or an external referral hospital. One respondent stated that "the lab staff tried their best to try and help us as far as possible with new innovative ways to provide us with the results as timeously as possible. I do, however, believe that more should be done to have backup systems in place should something like this happen in future." This highlights the importance of establishing clear protocols with the involvement of clinicians and management to ensure that the systems developed ensure clinical utility and patient safety.

ISO 15189 is an international standard outlining requirements for quality and competence in medical laboratories. The updated ISO 15189: 2022 emphasises risk-based approaches and patient-centred practices while promoting continuous improvement within clinical laboratories[11]. Additionally, it expands accreditation requirements for information systems, mandating that they be "implemented with cybersecurity considerations to prevent unauthorised access and protect data from tampering or loss" [12]. As described by Cassim and Chapanduka, the NHLS had limited resources to deal with the incident and required a longer time to develop contingency plans for result dissemination [7]. As a result of the increased reliance on manual processes, the laboratory could not maintain the same test turnaround times (TAT) as before the ransomware incident, which invariably increased. The perceived impact of this by clinicians included delays to elective and emergency surgery and to patient discharge. Ghafur et al. performed a retrospective analysis of the 2017 global ransomware attack, WannaCry, and its impact on the National Health Service in England. They reported 9% fewer elective admissions during this time and 13,500 cancelled outpatient appointments across the affected facilities. They further estimated a total economic loss of £5.9 million due to the cyberattack resulting from the loss of hospital activity during this time [13]. To streamline operations and alleviate pressure from increased manual processes, NHLS expert committees compiled and disseminated essential test lists (7). The survey responses indicate that clinicians reduced non-priority testing during the period of the ransomware attack. The use of two contrasting sentinel analytes in this study was intended to provide a pragmatic illustration of prioritisation behaviour during downtime rather than a comprehensive assessment of laboratory utilisation patterns. The decline in creatinine testing compared to previous years highlights the decreased utilisation of laboratory services during this time. Additional research on the financial impact of the ransomware attack we experienced would be valuable for understanding its broader consequences and creating strategies to prevent future incidents. By examining these impacts, we can develop policies that reinforce operational stability, ensuring that patient outcomes remain a priority, even in unforeseen and challenging circumstances.

Seventy-three percent of respondents reported that the ransomware attack impacted decisions around initiating or discontinuing patient treatment. This highlights the disruption to clinical decision-making and patient care, with one respondent noting that "It was incredibly difficult to treat critically ill patients timeously". Flavin et al. highlighted the effects of a national cyberattack and its impact on radiation therapy services in the Republic of Ireland in 2021, noting that 513 patients nationwide experienced interruptions in their treatment [14]. This illustrates the impact that cyberattacks can have on critical healthcare services. Unfortunately, no responses were received from oncology services in our study, preventing the review of the perceived impact on their operations. A study by Neprash et al reviewed ransomware attacks on healthcare delivery organisations in the United States from 2016 to 2021. Of the 374 attacks during this period, 166 (44.4%) resulted in disrupted care delivery, with 38 (10.2%) specifically leading to delays or cancellations of scheduled care [15]. These findings further highlight the widespread and multifaceted challenges ransomware attacks pose to healthcare systems.

The ransomware attack caused disruptions by increasing TAT and the unavailability of results on electronic web portals forced clinicians to physically collect hard copies of laboratory reports if the laboratory was unavailable to relay the result telephonically due to staff constraints. This additional burden significantly increased stress levels among clinicians already facing extended working hours. In South Africa, burnout

among healthcare professionals is a well-documented issue. A study in 2010 by Rossouw et al. assessed burnout and depression among medical doctors in healthcare facilities in the Western Cape, South Africa. Of the 132 doctors surveyed, 76% experienced burnout. Long working hours were identified as a major contributing factor, emphasising how the ransomware attack potentially exacerbated an already critical issue in the South African healthcare sector [16]. Although our study did not directly measure burnout, increased stress levels and longer working hours were found, which are important factors that contribute to clinician burnout.

A key contribution of this study is its focus on clinicians' experiences during a laboratory ransomware incident in a resource-limited setting of Sub-Saharan Africa. While several studies discuss healthcare cyberattacks and laboratory responses, few have examined the unique challenges clinicians face during such incidents. This perspective enhances our understanding of the impact on patient care in contexts where backup systems and resources may be limited.

Several limitations of this study should be acknowledged. The exact response rate could not be determined due to the electronic distribution strategy, which made it difficult to establish how many clinicians were reached or viewed the survey. In addition, response rates were lower among medical interns, a group heavily involved in result retrieval during the downtime period, potentially resulting in an incomplete representation of certain operational challenges. The overall sample size was relatively small, which may limit the generalisability of the findings, although the responses obtained nonetheless provide valuable and diverse insights from clinicians working in this setting.

From a laboratory perspective, test volume analysis was limited to two analytes and was not intended to reflect overall laboratory utilisation. This approach was chosen to provide a focused illustration of prioritised versus non-prioritised test requesting behaviour during the ransomware-related downtime. Finally, the study did not include objective patient safety outcomes, an important area for future investigation to better quantify the downstream clinical impact of such incidents.

Conclusion

This study provides valuable insights into clinicians' perceptions of the impact of a laboratory ransomware attack, highlighting the critical role of information systems in healthcare and their particular vulnerabilities in resource-limited settings. As one respondent aptly observed, "This was a terrible time in NHLS history, and it showed how much we rely on PC systems." The findings emphasise the urgent need for investment in both robust cybersecurity infrastructure and comprehensive contingency planning to ensure patient safety and minimise disruptions during future incidents. This imperative is especially critical considering global trends that show increasing frequency and sophistication of ransomware attacks specifically targeting healthcare services. Healthcare institutions must prioritise developing resilient systems that can maintain essential laboratory services even when primary information systems are compromised, particularly in settings where resources for rapid response may be constrained.

Acknowledgements

The authors extend their heartfelt gratitude to the clinicians of Tygerberg Hospital for their unwavering support and understanding during the challenging downtime period.

CRediT Author statements

All authors contributed to the conceptualisation, methodology, writing and review of the manuscript. AF performed the formal statistical analyses and generated the visualisations.

Data availability

Upon reasonable request, the data from the present study is available from the corresponding author.

Funding

None.

Conflicts of interest

None declared by the authors.

References

1. Almunawar MN, Anshari M, Almunawar MN. Health Information Systems (HIS): Concept and Technology [Internet]. 2012. Available from: https://www.researchgate.net/publication/221710863
2. Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Vol. 8, Digital Health. SAGE Publications Inc.; 2022.
3. Frisch NK, Gibson PC, Stowman AM, Goodwin A, Schwartz M, Cortright V, et al. Anatomy of a Cyberattack. Am J Clin Pathol. 2022;158(1):18–26.
4. Goodwin A, Wilburn C, Wojewoda C, Mesec J, Cacciatore LS, Grove SA, et al. Anatomy of a Cyberattack: Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime. Am J Clin Pathol. 2022;157(5):653–663.
5. Forsman RW. Why is the laboratory an afterthought for managed care organizations? Clin Chem. 1996;42(5):813–816.
6. About Us - National Health Laboratory Service [Internet]. [cited 2025 Feb 17]. Available from: https://www.nhls.ac.za/about-us/
7. Cassim S, Chapanduka ZC. Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations. SAMJ. 2024;e2549. Available from: https://samajournals.co.za/index.php/samj/article/view/2549
8. Duffy C, Murray C, Boran G, Srinivasan R, Kane A,

Leonard A. Survey of Laboratory Medicine's national response to the HSE cyberattack in the Republic of Ireland. Ir J Med Sci. 2024;193(2):889–896.
9. Lippi G, Akhvlediani S, Cadamuro J, Danese E, García De Guadiana Romualdo L, Delacour H, et al. EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) recommendations for reinforcing cyber-security and managing cyber-attacks in medical laboratories. Clin Chem Lab Med. 2024.
10. Stowman AM, Cacciatore LS, Cortright V, McConnell J, Wilburn C, Bryant B, et al. Anatomy of a Cyberattack. Am J Clin Pathol. 2022;157(6):814–822.
11. ISO 15189. Medical laboratories – Requirements for quality and competence. Geneva: International Organization for Standardization; 2022.
12. Ilinca R, Luțescu DA, Chiriac IA, Hristodorescu-Grigore S, Stănescu-Spînu II, Ganea I, et al. Cybersecurity requirement of ISO 15189 - a simplified protocol for laboratories. Rev Rom Med Lab. 2023;31(3):157–162.
13. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med. 2019;2(1).
14. Flavin A, O'Toole E, Murphy L, Ryan R, McClean B, Faul C, et al. A National Cyberattack Affecting Radiation Therapy: The Irish Experience. Adv Radiat Oncol. 2022;7(5).
15. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873.
16. Rossouw L, Seedat S, Emsley RA, Hagemeister D. The prevalence of burnout and depression in medical doctors working in the Cape Town Metropolitan Municipality community healthcare clinics and district hospitals of the Provincial Government of the Western Cape: a cross-sectional study. South African Family Practice. 2013;55(6):567–573.

Supplementary file

Supplementary Table 1: Participant Information Leaflet and Consent Form.

Title of Research Project **"Clinician Experience on The Impact of a Ransomware Attack on a Chemical Pathology Laboratory in South Africa"**	
Details of Principal Investigator (PI) / Researcher(s)	
Title, first name, surname Dr Ameerah Davids Dr Aaqilah Fataar	**Ethics reference number** N24/08/095
Full postal address Division of Chemical Pathology, 9th Floor Tygerberg Hospital, Francie van Zijl Drive, Parow, Cape Town	**PI Contact number** 082 585 8656; 082 568 6098

We would like to invite you to take part in this research project. We are a group of researchers from the Division of Chemical Pathology at Stellenbosch University, including consultants and registrars.

Please take some time to read the information presented here, which will explain the aims of this project. It is especially important that you are completely satisfied and clearly understand what this research entails and what your involvement entails. Also, your participation is **entirely voluntary**, and you are free to decline to participate.

The Health Research Ethics Committee at Stellenbosch University has approved this study [study number to be added]. The study will be conducted according to the ethical guidelines and principles of the international Declaration of Helsinki (2013), the South African Guidelines for Good Clinical Practice (2006), the Medical Research Council (MRC) Ethical Guidelines for Research (2002), and the Department of Health Ethics in Health Research: Principles, Processes and Studies (2015).

What is this research study all about?

Ransomware is defined as a "type of malware attack in which the attacker locks and encrypts the victim's data, important files; this may be followed by demands of payment to unlock and decrypt the stolen data". Ransomware attacks in the healthcare sector, including clinical laboratories, seem to be on the increase. It is crucial to understand the impact of these attacks on clinical services by getting feedback directly from clinicians.

This study aims to get feedback on the experience of clinical staff on the recent Information System (IT) downtime at the National Health Laboratory Service (NHLS) due to a ransomware attack. We seek to understand how this impacted the clinicians in performing their daily duties.

Why are you invited to participate?

You are invited to participate because you are a doctor working at Tygerberg Hospital.

Will you benefit from taking part in this research?

You will not directly benefit from this study; however, the findings may be used to design and amend current operating procedures for unplanned future downtime at Tygerberg laboratories.

Are there any risks involved in your taking part in this research?
There is no risk associated with this study.

Are there any costs involved if I decide to participate/take part?
There is no cost to you for participating in this project.

You can contact the Principal Investigators of this study, Dr Ameerah Davids or Dr Aaqilah Fataar on the phone numbers above or via email at adavids@sun.ac.za or aaqilah.fataar@nhls.ac.za if you have any questions about this study or encounter any problems.
You can phone the Health Research Ethics Committee at 021 938 9677/9819 if there still is something that concerns you about how this study is being conducted, or if you have a complaint.
You can download a copy of this information and consent form for you to keep safe.

Declaration by participant
By electronically signing below, I agree to take part in a research study entitled **Clinicians' Perspectives on the Impact of a Ransomware Attack on the Chemical Pathology Laboratory at a Tertiary Hospital in South Africa**

I declare that:
I have read this information and consent form, and it is written in a language in which I am fluent and with which I am comfortable.
I understand that taking part in this study is voluntary, and I have not been pressurised to take part.
I may choose to withdraw from the study by discontinuing to complete this electronic form.
Once I have electronically signed and submitted this form, I will not be able to withdraw from the study
My personal identifying information is not included in this study and therefore my responses cannot be linked back to me.
By clicking SUBMIT you are confirming that you are over 18 years old and have read and understood the above explanation about the study, and that you agree to participate. You also understand that your participation in this study is strictly voluntary.

Survey
Demographic questions

Are you currently employed at Tygerberg Hospital?
- Yes
- No

Were you employed at Tygerberg Hospital after the 1st of April 2024?
- Yes
- No

What is your current job title?
- Medical Intern
- Medical Officer
- Registrar
- Consultant/Fellow
- Head of Department

How many years of clinical experience do you have?
- 0-3 years
- 4-7 years
- 8-10 years
- More than 10 years

In which clinical setting do you predominantly work?
- Inpatient care
- Outpatient care
- Inpatient and outpatient care

In which division do you work?
- Medical intern rotating through multiple disciplines
- Internal Medicine
- Surgery
- Obstetrics and gynaecology
- Orthopaedics
- Anaesthetics
- Psychiatry
- Family medicine
- Emergency medicine
- Trauma
- Nephrology
- Haematology
- Oncology
- Other
- Paediatric
- Critical Care (ICU)

Did you scale down lab testing using the critical test list that was made available?
- Yes
- No

What was the most effective way that you obtained patient results?
- Collecting physical copies
- Single patient viewer
- Calling for results
- Other (please state)

Inpatient and outpatient questions/Inpatient only questions

	Agree	Somewhat Agree	Neutral	Somewhat disagree	Disagree
Downtime resulted in delay to diagnosis					
Downtime affected patient treatment decisions (initiation/ discontinuation)					
Downtime affected special investigations (e.g. CT scan/ imaging)					
Downtime affected patient referral					
Downtime affected elective surgery time					
Downtime affected emergency surgery time					
Downtime resulted in more frequent patient testing/ sampling					
Downtime delayed patient discharge (length of stay)					
Downtime led to longer working hours					
Downtime increased my level of stress at work					
The lack of specialised testing affected patient testing					

Outpatients only

	Agree	Somewhat Agree	Neutral	Somewhat disagree	Disagree
Downtime resulted in delay to diagnosis					
Downtime affected patient treatment decisions (initiation/ discontinuation)					
Downtime affected special investigations (e.g. CT scan/imaging)					
Downtime affected patient referral					
Downtime affected elective surgery time					
Downtime resulted in more frequent patient testing/sampling					
Downtime led to longer working hours					
Downtime increased my level of stress at work					
The lack of specialised testing affected patient testing					
Downtime led to longer patient waiting times					

Lab experience

	Agree	Somewhat Agree	Neutral	Somewhat disagree	Disagree
The Chemical Pathology laboratory was helpful					
The Chemical Pathology laboratory was prepared for the unexpected downtime					
The Chemical Pathology laboratory communicated critical results timeously					
Communication from the Chemical Pathology laboratory was effective					
The ward box system was effective for obtaining results					
The Chemical Pathology laboratory attempted to mitigate delayed turnaround times					
Requested Chemical Pathology results were often lost					
Chemical Pathology laboratory results issued during downtime were user friendly					
Lack of auto calculations (e.g. eGFR, urine protein creatinine ratio, transferrin saturation etc.) made result interpretation more challenging					
Lack of reference intervals made result interpretation more challenging					
Lack of interpretive comments made result interpretation more challenging					
The Chemical Pathology patient results were trustworthy during downtime					