Comment on: 'Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations'

To the Editor: In their article on the National Health Laboratory Service (NHLS) cyberattack, Cassim and Chapanduka[1] suggest that the use of platforms such as Gmail and WhatsApp to transmit patient data *may* have violated the Protection of Personal Information Act 4 of 2013 (POPIA).[2] However, this critical legal question is left unresolved in their analysis. More notably, the authors call for new national legal policies without first analysing how the existing legal framework applies to such situations – and indeed offers solutions.

Section 19 of POPIA requires that a *responsible party* – in this case, the NHLS – implement appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised access to personal information, especially sensitive health data. Crucially, POPIA's obligations remain in force during a data breach; if anything, the duty to protect personal information becomes more acute during such events. A security breach cannot justify lower standards; rather, it should trigger an intensified effort to uphold them.

The NHLS should have had a contingency plan that accounted for this scenario. In its absence, immediate consultation with legal professionals experienced in data protection was imperative. Practical measures, such as password-protecting files sent via Gmail, would have constituted reasonable technical safeguards under POPIA, given the circumstances. The article does not indicate whether any such steps were taken, raising concerns about the adequacy of the NHLS's data protection practices during the incident.

Furthermore, POPIA's chapter 4 provides for *exemptions* if these involve 'a clear benefit to the data subject … that outweighs, to a substantial degree, any interference with the privacy of the data subject …', offering a legal pathway when conventional data protection measures are impractical owing to emergencies.[3] The Information Regulator has issued clear guidance on how to apply for such exemptions.[4] It appears that the NHLS did not pursue this option. An exemption application could have been urgently processed, providing clear, tailored legal conditions for data handling during the crisis. This could have allowed laboratory professionals to communicate results in unorthodox ways to avoid patient harm, without violating the law.

We respectfully suggest that the call for new national legal policies is misplaced. What is needed is not legal reform, but effective operationalisation: a legally informed contingency plan, the timely use of exemption mechanisms, and practical safeguards – even under pressure.

Acknowledgment. ChatGPT was used to improve language and readability.

D W Thaldar
School of Law, University of KwaZulu-Natal, Durban, South Africa
thaldard@ukzn.ac.za

W Preiser
Division of Medical Virology, Stellenbosch University and National Health Laboratory Service, Tygerberg Hospital, Cape Town, South Africa

1. Cassim S, Chapanduka ZC. Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations. S Afr Med J 2024;114(12):e2549. https://doi.org/10.7196/SAMJ.2024.v114i12.2549
2. Protection of Personal Information Act 4 of 2013. https://www.gov.za/documents/protection-personal-information-act (accessed 5 February 2025).
3. POPIA: Protection of Personal Information Act. Chapter 4. Exemption from conditions for processing of personal information. https://popia.co.za/protection-of-personal-information-act-popia/chapter-4 (accessed 5 February 2025).
4. Information Regulator (South Africa). Protection of personal information. Who should be registered as an Information Officer? https://inforegulator.org.za/popia (accessed 5 February 2025).

Response to letter regarding 'Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations'

To the Editor: We thank Thaldar and Preiser for their letter in response to our article.[1] We welcome the opportunity to clarify the following aspects of the article.

1. The National Health Laboratory Service (NHLS) did indeed secure an exemption from the Information Regulator, in view of the fact that aspects of the Protection of Personal Information Act 4 of 2013 (POPIA)[2] had to be violated in pursuit of public benefit. That public benefit, in this case, included preservation of life and limb. However, as we did not know exactly when the exemption was granted, we believe that our wording is measured and fair to the NHLS. Furthermore, the well-intentioned use of *sensu stricto* illegal channels of private data communication by NHLS rank and file cannot be scientifically excluded, especially in the early part of the cyberattack.
2. The 'national and legal policies'[1] we propose as future requirements do not relate to POPIA. They relate to all other legal aspects that are involved in the prevention of and response to future cyberattacks and other threats, which we regard as inevitable.

All other omissions regarding the details of the response are due to the concision that must be applied in writing articles of this nature. It remains our sincere hope that the recommendations we made will help formulate preparedness policies, strategies and tactics pertaining to future NHLS operational threats.

S Cassim, Z C Chapanduka
Division of Haematology, Department of Pathology, Faculty of Medicine and Health Sciences, Stellenbosch University and National Health Laboratory Service, Tygerberg Hospital, Cape Town, South Africa
sumaiya@sun.ac.za

1. Cassim S, Chapanduka ZC. Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations. S Afr Med J 2024;114(12):e2549. https://doi.org/10.7196/SAMJ.2024.v114i12.2549
2. Protection of Personal Information Act 4 of 2013. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (accessed 27 February 2025).

S Afr Med J 2025;115(5):e3101. https://doi.org/10.7196/SAMJ.2025.v115i5.3101