



Health

Dr Juanita Fernando
Chair, Health Committee
Australian Privacy Foundation
Email: juanita.fernando@privacy.org.au

Our ref S21/252

Dear Dr Fernando

Thank you for writing about the NSW Health Accellion cyber-attack. I regret the delay in responding.

I acknowledge your concerns and appreciate your interest in this matter.

NSW Health appreciates the evolving cyber security risks and continuously strengthens protections to ensure safe operation of the public health system and safeguard the privacy of our patients.

I can assure you that NSW Health's core information systems, such as electronic medical records, were not compromised in this attack. The software involved, Accellion FTA, is no longer used by NSW Health.

NSW Health has been working closely with Cyber Security NSW, who are coordinating the whole of government response to this incident and with NSW Police, who are undertaking an investigation.

The privacy of individuals is important to NSW Health, and we are contacting individuals impacted by the attack, so they can take appropriate precautions and access support. A cyber incident help line has been established to provide further information, advice and support to impacted individuals.

NSW Health has robust measures in place to manage cyber security risks. NSW Health is compliant with the NSW Government's Cyber Security Policy, which mandates annual attestation of the maturity of NSW Health's security posture. eHealth NSW, NSW Health's ICT agency, has a dedicated information security services team who develop information security policies and procedures, monitor their use across the system and respond to cyber security threats and incidents across the health system.

NSW Health also has a Health Security Operations Centre, operated by a world-leading cyber security vendor, that provides continuous real time threat intelligence and cyber-attack monitoring across NSW Health Systems. This enables early detection and rapid response to threats to minimise any adverse impacts. Cyber security training is also mandated for all NSW Health employees to ensure they are aware of their responsibilities in relation to information privacy and security.

In April 2021, the NSW Government approved NSW Health's business case for a cyber security uplift program of work. Funding has been allocated to NSW Health to increase its level of maturity against the Australian Cyber Security Centre's 'Essential 8' core mitigation strategies, and this work is well underway.

NSW Ministry of Health

ABN 92 697 899 630

1 Reserve Road, St Leonards NSW 2065

Locked Mail Bag 2030, St Leonards NSW 1590

Tel (02) 9391 9000 Fax (02) 9391 9101

Website: www.health.nsw.gov.au

Thank you again for writing. For more information, please contact Dr Zoran Bolevich, Chief Executive, eHealth NSW and Chief Information Officer, NSW Health at Zoran.Bolevich@health.nsw.gov.au

Yours sincerely

A handwritten signature in black ink, appearing to read 'E Koff', written in a cursive style.

Elizabeth Koff
Secretary, NSW Health

A handwritten date in black ink, '29/8/21', written in a cursive style.