NSW Health

Frontier Software cyber security incident

General Frequently Asked Questions (FAQs)

Who is Frontier Software and how does it involve NSW Health?

Frontier Software provided payroll software to NSW Health between 2001 and 2015. In 2022, Frontier Software notified NSW Health that a cyber-attack in November 2021 included the payroll information of approximately 1600 employees. Frontier Software retained relevant payroll data in an archived system to enable data retrieval by HealthShare NSW on an as needed basis.

Why does Frontier Software have my personal employee information?

All organisations providing payroll services require access to personal information in order to make salary payments and meet Australian Taxation Office reporting obligations.

Frontier Software is required to comply with a range of contractual and legislative requirements regarding the protection of personal information provided to it by NSW Health.

Is NSW Health still using this software?

No. In 2015, NSW Health replaced this software with StaffLink.

Who is impacted by the data breach?

The breach is limited around 1600 staff who were employed by the Ministry of Health, as a Senior Executive of NSW Health, or in the Mental Health Review Tribunal, Health Professional Councils Authority, Official Visitors Program, Health Infrastructure, and the previous NSW Institute of Psychiatry between 2001 and 2015.

The breach does not affect any non-executive current or former staff who have been employed exclusively through local health districts and public hospitals.

Frontier Software cyber security incident | General Frequently Asked Questions (FAQs)

What personal information was accessed?

The data accessed was payroll information of current and former NSW Health employees. The following key types of personal information may have been included in the impacted data:

- Name
- Residential address and telephone
- Date of birth
- Tax file number
- BSB and financial institution (bank) account number

How can I find out if I have been impacted?

Current NSW Health staff who have been impacted by the breach are being notified via email.

If you were employed at the above entities between 2001 and 2015, but are no longer employed within NSW Health, please contact the dedicated help line on 1300 679 367 (option 9).

Why is the risk of data theft considered low?

Frontier Software informed NSW Health that they took immediate steps to prevent any further access to the data, prevent it being published on the dark web, and to protect against it being misused either now or in the future. Ongoing monitoring confirms that no data from the breach has been uploaded to the dark web.

What has Frontier Software done to date?

Frontier Software worked with external cyber security and forensic specialists to assist their internal Frontier Software team to contain the incident, recover their systems, strengthen their security and investigate the breach. Frontier Software reported the incident to the Office of the Australian Information Commissioner (OAIC), the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP) and relevant state police.

Where a tax file number (TFN) has been accessed, Frontier Software informed the Australian Tax Office so they can apply additional security measures and monitor for any potential misuse of that TFN. Please be aware that these measures may impact access to your myGov account, but this is all with a view to providing additional protection. For further information contact the ATO Client Identity Support Centre on 1800 467 033 Monday to Friday 8:00 am–6:00 pm AEST or visit the ATO website for data breach guidance.

Frontier Software has also alerted Services Australia to the incident. Where impacted information includes information for which Services Australia is responsible, Services Australia has added additional security measures to protect those details where relevant.

Why are impacted employees only being notified now?

Upon discovering the cyber-attack, Frontier Software immediately began investigating the incident. Between November 2021 and now, an extensive amount of work has been undertaken together with Frontier Software's external cyber advisors to determine precisely whose and what information was impacted. This has included undertaking a detailed manual review of the impacted data to identify all potentially impacted persons. NSW Health then needed to compare this data with its own data to obtain, where possible, up to date contact details of impacted individuals.
This has been a complex and time-consuming exercise, complicated by the volume and largely unstructured nature of the data and the need to ensure in identifying, cataloguing and matching the data. Having completed this very detailed exercise, we can confirm that you were impacted.

What support is available for those impacted?

If you are concerned about the potential misuse of your personal information, Frontier has arranged free support from IDCARE, Australia's national identity and cybersecurity community support service.

If you are an impacted person and wish to access IDCARE's services, please contact NSW Health's dedicated help line on 1300 679 367 (option 9).

What can I do to protect myself?

IDCARE's Learning Centre contains information and resources on protecting your personal information.

Please remain alert to any increased scam activity, especially email and SMS or telephone phishing scams (i.e., fraudulent communications disguised as if to look like they come from an organisation you trust) and, in particular any such scam activity purporting to come from Frontier or NSW Health.

Further information on online safety, cyber security and helpful tips to protect yourself and respond to scams, identity theft and other online risks, can be found at the following government agency websites.

- Australian Cyber Security Centre
- Scamwatch

If you would like more information about how NSW Health protects the personal information of our staff and our information management and internal review procedures, please refer to the Privacy Leaflet for Staff.