NSW Health

Frontier Software cyber security incident

Email notification to impacted current staff

Dear **<<First Name>>**

Frontier Software cyber security incident

I am writing to notify you of a cyber-attack and data breach that has involved some of your personal information held by Frontier Software (Frontier).

I want to make clear that in the circumstances surrounding this breach, we are advised by Frontier that it is very unlikely that the information is in possession of the organisation that stole the information and there have been no reports of any misuse of the information.

NSW Health is communicating to you for an abundance of caution and to advise you of the support services Frontier has put in place – again for an abundance of caution.

Frontier were the providers of the Chris21 payroll system used by the Ministry of Health and some small entities prior to the introduction of StaffLink in 2015. Frontier retained relevant payroll data in an archived system to enable data retrieval by HealthShare NSW on an as needed basis. Frontier informed NSW Health in late July 2022 that data containing personal information of current and former employees of the Ministry of Health or whose payroll was processed by the Ministry of Health was downloaded from its systems in a cyber-attack in November 2021.

Frontier 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.

Frontier Software cyber security incident | Email notification to impacted current staff

NSW Health has undertaken an extensive amount of work with Frontier's external cyber advisors to determine precisely whose information was impacted by the breach. Having completed this very detailed exercise to identify, catalogue and match the data, we can confirm that you were impacted by the initial breach, noting that Frontier took immediate action to minimise risks arising for individual's whose personal information was breached.

Based on the actions undertaken and advice provided, we consider that there is a significantly reduced risk associated with this data breach, but we nevertheless consider it important to inform you that the breach occurred.

Frontier has reported the incident to the Office of the Australian Information Commissioner (OAIC), the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP), NSW Police and the Australian Tax Office. The Ministry of Health has notified the NSW Privacy Commissioner.

The incident did not involve any of NSW Health's core systems, current payroll system or impact on any patient information, health or hospital records.

I appreciate that this may be distressing for you and Frontier has organised for support to be available at no cost by contacting IDCare on 1800 595 160 and providing the referral code of "FDI2-ID". IDCare is an independent organisation that specialises in identity protection and can provide advice and services to persons who may have concerns about possible future impacts. The attached information sheet provides more details about what happened, the particular type of personal information involved, the steps taken to date and the steps that you can take to reduce any potential impact on your personal information.

If you would like any more information about the data breach, assistance updating other personal details, please contact the dedicated NSW Health helpline on 1300 679 367. Alternatively, you may contact Frontier Software directly by email at cyberhelp@frontiersoftware.com.au or by calling 1300 007 446.

Yours sincerely

Phil Minns,
Deputy Secretary
People, Culture and Governance