# WRITTEN STATEMENT

# BY

# THE WELSH GOVERNMENT

|  |  |
| --- | --- |
| **TITLE** | ***Landauer Data Breach*** |
| **DATE** | ***12 July 2017*** |
| **BY** | ***Vaughan Gething, Cabinet Secretary for Health, Well-being and Sport*** |

On 17 March, I published a written statement on the cyber security attack on Landauer, the third party company providing the Radiation Protection Service for Velindre NHS Trust, on behalf of NHS Wales, which resulted in some personal information of staff being accessed illegally.

In that statement, I outlined the action being taken in response to the Landauer incident, along with the wider reviews that would be undertaken as a result of it. As I said I would, I am issuing this written statement to provide an update now that NHS investigations have been completed.

Firstly, I can confirm that all identified affected NHS Wales staff have been notified and offered support. The support included guidance on monitoring their financial affairs; via telephone, email and drop-in sessions; and, free access to the Experian credit check service for two years. Health boards and trusts have also provided assurance to staff who were not affected by the breach, but who may have been concerned that they were.

Although considerable effort was made, there remain a number of individuals who could not be contacted because there was insufficient detail available to identify them.

In addition to the investigation undertaken within Velindre NHS Trust, which delivered a full incident report, I requested that a data breach review group be established to review the breach and take action to ensure future assurance. This group included representation from Welsh Government, NHS Wales Informatics Service (NWIS) and Velindre NHS Trust.

As a result of the work of the data breach group:

* A review of all nationally hosted systems which are either hosted by, or accessed by, third party providers has been undertaken and mitigating controls have been put in place to address any future risk;
* The Director General for Health and Social Services/ NHS Wales Chief Executive has written to NHS Wales Chief Executives reminding them of the need to have contractual controls in place relating to information governance and information security for third party suppliers;
* The NHS Wales Informatics Service cyber incident response plan is being applied for any cyber security incidents across Wales. This ensures that standard processes will be deployed across NHS Wales in the event of a cyber security incident, ensuring that incidents are reported, communicated and escalated appropriately. The NHS is working to align local cyber incident response plans to the national template; and
* *A* group led by NWIS and Senior Information Risk Owners is reviewing current practice and will advise on further developments. Each Health Board and Trust in Wales now has a board-level executive fulfilling this function as the person responsible for information risk management.

A review by the Information Commissioner’s Office is ongoing and the findings will be published in due course.

This data breach, as well as the recent ransomware cyber attack, has reminded us of the need to remain vigilant, ensure that we take the appropriate precautions and be ready to respond.