Cyber attack update

Please share this leaflet with the other people in your household. If you need this leaflet in another language or format, telephone 01387 272 733 or email dg.patientservices@nhs.scot. Please see over the page for an Easy Read version of this message.

From Julie White, Chief Executive, NHS Dumfries and Galloway

In February this year, NHS Dumfries and Galloway was the victim of a targeted attack by cyber criminals. This did not interrupt the care provided to patients, and no data on our systems was deleted or changed.

However, the criminals were able to access and copy large amounts of patient and staff-identifiable data. When their demands weren't met, they published the stolen files onto the internet on May 6 2024.

We are advising people in Dumfries and Galloway that the best approach to take is to assume that some data relating to you is likely to have been copied and published. This is an extremely serious situation, and everyone is asked to be on their guard for any attempts to access their computer systems, or any approaches by anyone claiming to hold their data or someone else's data.

This leaflet sets out the type of data which was stolen, potential risks associated with this, the measures which you might want to consider taking in response, and information on how we can support you.

What data was published?

The millions of pieces of data copied and published are generally very small, individual files: for example, x-rays, test results and correspondence between health and social care teams, correspondence between our teams and patients, and complaints letters.

The volume of data stolen and the challenge of analysing it means a decision was taken to prioritise 'high-risk' data which generally relates to most vulnerable patients. If you are part of a high-risk group which represents a small number of people living in our communities, and we believe the publication of the stolen data represents an additional risk to you, we will be in touch with you to discuss this. As our investigations are ongoing, we will not be able to tell people what specific data has been published about them.

What are the risks?

The following have been identified as potential risks resulting from the publication of the data, and further information and support is available via the website and helpline detailed below:

Identity theft.

This concern is more for NHS staff than for patients, because of the sort of information gathered from staff during the recruitment process. NHS staff have been notified of this risk, and have been provided with advice.

Action Fraud provides information on identity fraud and theft at this web address: https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft

The National Cyber Security Centre has published advice on actions following a cyber attack which can be found at this address:https://www.ncsc.gov.uk/guidance/data-breaches

Security.

Since the cyber attack, we have been asking both staff and the public to be on their guard for any suspicious activity. This includes any attempts to access computer systems, such as suspicious emails from an unverified sender asking them to click a link (known as 'phishing'), as well as phone calls. If anyone has suspicions, they should call Police Scotland by phoning 101. Passwords should be changed regularly as a matter of course, but people may want to ensure that their passwords have been updated. Strong, unique passwords should be employed, such as a combination of three random words. Where information may be held for staff on how to gain access to a property, patients have been notified and changes implemented.

Extortion.

It is an acknowledged risk that the stolen data could be used to exploit or threaten people. This could either be by the cyber criminals who copied the data or someone who accesses it now that it has been published. Anyone accessing the stolen data would be in breach of the Data Protection Act. If you receive a suspicious approach from anyone claiming to possess your NHS data or anyone else's NHS data, you should call Police Scotland by phoning 101.

Anxiety.

NHS Dumfries and Galloway fully recognises the anxiety which may result from the copying and publication of confidential NHS patient and staff data. The situation is not unprecedented. In 2022, stolen medical records of more than 10 million people in Australia were posted online. The sheer scale of that data meant that the impact was limited, and it has been suggested by one prominent cyber security expert that this may also be the case in Dumfries and Galloway. A helpline set out below can provide signposting to support, including psychological support for those experiencing anxiety.

More information

More information is hosted online at the website www.nhsdg.co.uk/cyberattack

The helpline can be reached by calling 01387 216 777, Monday to Friday 9 am to 6 pm and Saturday 9 am to 1 pm.

The NHS Head of Information Governance can be contacted by emailing dg.dpa-office@nhs.scot

On behalf of NHS Dumfries and Galloway, I would like to apologise for the anxiety which may have been caused to you due to this situation. We have sought to be as open as possible while adhering to the very explicit guidance we have received from Police Scotland and partner agencies.

Julie White
Chief Executive, NHS Dumfries and Galloway