

> Retouradres: Postbus 91163, 3007 MD Rotterdam
<Initials client> <Name client>
<Adres client>

Utrecht, 12 August 2025

RE: data leak of personal data on participants in cervical cancer screening
Reference:

Dear Ms <name client>,

By this letter we want to inform you about a recent data leak involving your personal data. In the past, you took part in the population screening programme for cervical cancer. Your cervical smear test or self-test was processed in the laboratory Clinical Diagnostics NMDL (a Eurofins subsidiary) in Rijswijk. Hackers managed to gain access to the ICT systems of this laboratory. In the context of this data leak, the data of more than 485,000 participants in the cervical cancer screening programme were viewed and copied. That included your personal data.

We are deeply sorry that your data was involved in this data leak, and can imagine that you may have questions or uncertainties.

What types of data does this concern?

We have confirmed that it included personal data such as name, address, city, date of birth, citizen service number (BSN), test result(s) and the names of care providers. For a limited number of participants, it also included e-mail addresses or phone numbers.

Does not affect your test result

The data leak does not affect the result that you already received, or are going to receive. If you sent in a self-test or had a cervical smear test in the context of the cervical cancer screening programme, you do not have to repeat the test.

Clinical Diagnostics *only* processes the test samples from the cervical cancer screening programme for Bevolkingsonderzoek Nederland. This data leak did not affect any data on participants in the population screening programmes for breast cancer or colorectal cancer.

If you take part in cervical cancer screening from now on, participation is safe, because the self-tests and cervical smear tests will now be sent to the other two laboratories that we work with.

Always stay alert for fraud

Malicious agents may try to misuse personal data that was acquired illegally. It is important to always stay alert for possible fraud. Within the group of participants affected by this hack, there were a limited number of participants whose e-mail addresses or phone numbers were also included. We always recommend to stay alert to any possible form of misuse of your personal data. Details on what you can do if you think your data is being used by malicious agents can be found on Government.nl:
<https://www.government.nl/topics/cybercrime/forms-of-cybercrime>

Any questions?

We can imagine that you might have questions. Current updates on the situation will be posted on our website, as well as a FAQ (in Dutch): www.bevolkingsonderzoeknederland.nl/nieuws/datalek.

If your question is not answered in the FAQ, email us at vragenBMHK@bevolkingsonderzoeknederland.nl. You can also call us on: <phone number>
Clinical Diagnostics NMDL has also posted information about the data leak, a FAQ and contact details on its website (www.clinicaldiagnostics.nl).

We understand that this message may cause concern, and regret any inconvenience this may involve for you. We are doing everything in our power to keep this from happening again in the future.

Kind regards,

A handwritten signature in black ink, appearing to read 'Elza'.

Elza den Hertog
Executive Board, Bevolkingsonderzoek Nederland