FREQUENTLY ASKED QUESTIONS: SUSPECTED ACCELLION DATA BREACH

How did this data breach happen?

The information available at this stage indicates that there was a vulnerability in the Accellion software that allowed unauthorised users to gain access. The data held in Accellion is encrypted if accessed by anyone other than authorised users. However, the vulnerability allowed the unauthorised users to access unencrypted data by appearing to be legitimate users.

What files or information did the hackers access?

QIMR Berghofer's initial investigations indicate that about 4 per cent, or 620MB, of the Institute's files held in Accellion appear to have been accessed on 25 December 2020. We do not yet know which files may have been accessed. We have sent a copy of our system to Accellion, which is conducting a forensic analysis to confirm that a data breach has occurred, and if so, to identify which files were accessed.

QIMR Berghofer has been working with the Institute's 9 Accellion users to review the files that are held in it. These include data from clinical trials of anti-malarial drugs, CVs of about 30 current and former research staff, some internal documents, and documents being shared with the Mosquito and Arbovirus Research Committee.

QIMR Berghofer's initial investigations indicate that no personal identifying information belonging to members of the public was held in the Accellion system. While some personal information belonging to malaria clinical trial participants was in Accellion, there were no names or contact details, meaning that none of the information can be used to identify participants.

I participated in one of the malaria clinical trials. Do I need to be worried about my personal information?

Based on our initial investigations, we don't believe you need to be worried because the information held in Accellion is de-identified and therefore cannot be used to identify or contact you.

Some of the documents in Accellion include the initials, date of birth, age, gender, and ethnic group of clinical trial participants, as well as a de-identified participant code. Some other documents include participants' de-identified medical histories, along with the de-identified participant codes. No names or contact details of clinical trial participants were included in any of the documents that could potentially have been accessed.

These clinical trials are conducted with healthy volunteers.

If you participated in one of our clinical trials of an anti-malarial drug, we haven't been able to contact you because QIMR Berghofer has no record of your name or contact details and we cannot identify you from the files in Accellion. Your name and contact details were only collected by the clinical trial facility that recruited you.

While we don't believe that any of the information held in Accellion can be used to identify you, we apologise sincerely for any worry or inconvenience this data breach has caused you. QIMR Berghofer is very grateful to all of our study participants and want to assure you that data security is a high priority.

We are working with Accellion to determine which files may have been accessed and will provide an update on this page when we have that information.

If you are concerned, below is some information and advice on protecting your identity data:

- Know how to spot a scam. You are more likely to be targeted by scammers if they have your information. The more information they have, the more personalised they can make the scam. This increases their chances of being successful.
- ScamWatch have a mailing list available to receive information on the latest scams, as well as details on different scams and what to look out for.
- Enable multi-factor authentication for your accounts where possible.
- Ensure you have up-to-date anti-virus software installed on any device you use to access your emails.
- Do not open attachments or click on links in emails or social media messages from strangers or if you're unsure if the sender is genuine.
- Do not share your personal information until you are sure about who you are sharing it with. If someone calls you and claims to be from an agency or organisation, you can hang up and call the agency or organisation back using publicly available contact details (e.g. from their website or a phone book) to be sure you are really talking to a staff member from that agency or organisation.
- IDCare also provide free support services across Australia and New Zealand for those who have been the victim of a cybersecurity incident.

I have participated in another QIMR Berghofer study or clinical trial, do I need to be worried?

If you have participated in any other QIMR Berghofer studies or clinical trials – including QSkin, D-Health, or the Prospective Imaging Study of Ageing – you don't need to worry. No files or information from these studies are held in Accellion. The only files in Accellion that included de-identified information about human participants are from the Institute's anti-malarial drug trials.

When did QIMR Berghofer become aware of this suspected data breach?

The first information or advice QIMR Berghofer received from Accellion was in early January, when the company advised the Institute to apply a security patch. QIMR Berghofer immediately took the software offline and applied the patch.

QIMR Berghofer received further notifications from Accellion in January about vulnerabilities and patches and the Institute followed the company's instructions.

Accellion notified QIMR Berghofer on Tuesday 2 February 2021 that it believed the Institute had been affected by a data breach.

Why didn't QIMR Berghofer detect the breach when it occurred on Christmas day?

Because the unauthorised users appear to have exploited a vulnerability in the Accellion system, they appeared to be a 'legitimate' user.

In January, QIMR Berghofer followed Accellion's advice in applying security patches, and, as a precaution, reviewed the logs of file access, which appeared to be normal.

It was not until 2 February 2021 that Accellion advised QIMR Berghofer of the suspected data breach.

If the suspected data breach happened on Christmas day, why haven't you told us about it sooner?

QIMR Berghofer were not made aware of the possible breach until 2 February 2021.
QIMR Berghofer doesn't yet have confirmation that a data breach has definitely occurred, although it looks very likely. We also don't know at this stage which files were accessed and are waiting on Accellion to provide that information.

Because of that, over the last 9 days, we have been working with the different users to investigate all of the different files that are in Accellion and that could potentially have been accessed, and to find out whether there was any personal information in those files.

We have also notified the Office of the Australian Information Commissioner, the Australian Cyber Security Centre, and our stakeholders and clinical trial partners.

We didn't think it was appropriate to wait until we received confirmation from Accellion, so as soon as we had conducted a preliminary investigation to know what was in Accellion, we shared this information publicly.

What action has QIMR Berghofer taken since this data breach?

As soon as Accellion notified QIMR Berghofer of a likely data breach, the Institute immediately shut down the software and launched an internal investigation and forensic analysis. We have also sent a copy of our system to Accellion, which is conducting its own forensic analysis.

In the meantime, the Institute has been investigating which files were in Accellion so that we could notify anyone who may have been affected by the possible data breach.

QIMR Berghofer has decommissioned the Accellion system, which had been scheduled to occur next month.

The Institute is also looking at whether there are any additional measures that can be taken to protect data. This includes putting in place new procedures to try to ensure that any files in third-party file-sharing services are regularly reviewed and removed.

What is QIMR Berghofer doing to protect data it holds?

The Institute uses a wide range of cyber security measures, including firewalls, encryption, de-identifying data, and regular staff training.