Australian Government

Office of the Privacy Commissioner

Notifiable Data Breach Form

About this form

Notifiable Data Breach statement

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the Privacy Act 1988.

Part one is the 'statement' about a data breach required by section 26WK of the Privacy Act. If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

The OAIC encourages entities to voluntarily provide additional information about the eligible data breach in part two of this form. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

Before completing this form, we recommend that you read What to include in an eligible data breach statement.

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review Identifying eligible data breaches.

The OAIC will send an acknowledgement of your statement about an eligible data breach on receipt with a reference number.

You can save this form at any point and return to complete it within 3 days. To save your form, click on the Save For Later button on the top right-hand corner of this form. If you do not submit your saved form within 3 days, your saved information will be permanently erased.

Refreshing your browser will clear any information that you have not saved. If you need to refresh your browser while completing this form and wish to keep your changes, please save the form first.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles.

We collect this information to consider and respond to your breach notification. We may use it to contact you.

More information about how the OAIC handles personal information is available in our privacy policy.

Part one - Statement about an eligible data breach

About part one

The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required).

Organisation/agency details

You must complete this section

Organisation/agency name *

MannaCare Inc

Phone *

03 9856 1201

Email *

contact@mannacare.org.au

Address Line 1 *

371 Manningham Road

Address Line 2

Suburb *

Doncaster

State *

VIC

Postcode *

3108

Other contact details

Any queries should be directed to
Vanessa May
General Manager Corporate Services
Tel: 03 9856 1206
Email: vanessa.may@mannacare.org.au

Description of the eligible data breach

You must complete this section

A description of the eligible data breach: *

On 24 March 2021, MannaCare was advised by its external IT provider that there was a possibility that MannaCare had been a victim of the HAFNIUM cyber attack. This attack uses a vulnerability in Microsoft Exchange to gain 'back door' access to servers, enabling the hacker to plant malicious tools designed to extract data. MannaCare had already applied the relevant security patch released by Microsoft on 2 March 2021 in a timely fashion and had reasonably assumed that the threat of attack had been averted. However, it subsequently became apparent that this particular cyber attack had emerged overseas in early January 2021. As the release of the patch was not until March, there had been a significant window of vulnerability.

On 24 March 2021, MannaCare's IT security monitoring system detected some unexplained increase in CPU activity on its Exchange server. MannaCare was advised of this by its external IT provider and immediate steps were taken to investigate and mitigate the possibility of data loss. Servers were shut down whilst multiple scans were run on all servers. All recommended steps to detect signs of the HAFNIUM attack were performed. Two data extraction tools related to the HAFNIUM cyber attack were subsequently detected on the Exchange server, confirming the likelihood that MannaCare had in fact been attacked. This server is also the main file storage server for the organisation. The malicious files were removed. Multiple scans, using a variety of tools, were performed on all servers and on all work stations. This was performed over several days. No further malicious files were found and there is no evidence of any remaining threats. Review of historical backups show that the Exchange server was compromised some time between 28 February 2021 and 5 March 2021.

There is no way of determining definitively whether any data was extracted and there is certainly a possibility that there has been no data theft. Additionally, MannaCare has not been approached by any group or individual demanding a ransom for any stolen data. However, the two malicious files found are specifically designed to extract data. Although there is no evidence to date of any data theft and the probability of data theft relating to any one individual is negligible, due to the large number of potential individuals impacted and the type of data which may have been taken, MannaCare has determined that, acting in an abundance of caution, a breach that could result in serious harm to one or more individuals should be considered likely. There is no way of identifying the cyber criminals responsible for this attack.

Although all known steps required to prevent a further HAFNIUM attack have been undertaken, general cyber security measures have also been reviewed and strengthened. Network password policy was amended to mandate a high degree of complexity; all MannaCare network users were required to change their passwords; workstation protection has been increased; storage time of backups has been extended; and network system logs duration has been increased to provide an increased time window for tracking of potential hacking attempts.

MannaCare has a reasonably high degree of multi-layered cyber security protection in place on all its servers and workstations. Unfortunately, the HAFNIUM attack has taken the world by surprise. This criminal group has predominantly targeted organisations in the health industry and several thousand organisations across Australia and other countries have been attacked.

Information involved in the data breach

You must complete this section

Kind or kinds of personal information involved in the data breach: *

Although there is no evidence of data theft, the types of personal information that may have been stolen include:
- Email account information of MannaCare staff.
- Staff files, including contract information, taxation declaration forms, and other employment documentation.
- Contact information of clients, client family members, suppliers, and staff.
- Health information relating to clients, including medical diagnoses, health assessments, medication, care plans.
- Client medicare numbers, pension numbers, DVA information.

In addition, please select any categories that apply:

- [ ] Financial details
(e.g. credit card number, transaction history, credit report)
- [x] Tax File Number (TFN)
- [x] Identity information
(e.g. Centrelink Reference Number, passport number, driver license number)
- [x] Contact information
(e.g. home address, phone number, email address)
- [x] Health information
- [ ] Consumer Data Right (CDR) information
(e.g. information about banking customers sent/received via the CDR regime)
- [ ] Other sensitive information
(e.g. sexual orientation, political or religious views)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach: *

- Change email account passwords, using strong passwords not used for any other accounts.
- Enable multi-factor authentication on email accounts if possible.
- Keep an eye out for scam emails
- Have up-to-date anti-virus software installed on all devices used to access emails.
- Do not open attachments or click on links in emails or social media messages from strangers or if you are unsure if the sender is genuine.
- Do not share personal information over the phone unless you are sure who you are talking to.
- If you are called by someone claiming to be from an organisation or agency and you have any doubts you can let them know you will call them back to confirm their identity. Make sure you use an independent source such as a website or published phone book to obtain their phone number.
- You can contact relevant government agencies if you have concerns or questions around identity documents (e.g. Medicare)
- Further information on steps you can take can be found on the Office of the Australian Information Commissioner (OAIC) website. Visit https://www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification/

Other entities affected

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation/agency affected?

- ( ) Yes
- (•) No

Part two - Additional information

About part two

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

Your contact details

Title

Mrs

First Name

Vanessa

Last Name

May

Phone

03 9856 1206

Email

vanessa.may@mannacare.org.au

Breach details

Date the breach occurred

You may provide your best estimate if the exact date is not known:

01 Mar 2021

Date the breach was discovered

You may provide your best estimate if the exact date is not known:

23 Mar 2021

Primary cause of the data breach

- (•) Malicious or criminal attack

  A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.

- ( ) System fault
- ( ) Human error
- ( ) Other
- ( ) Currently unknown

Please provide more detail by selecting one of the following:

- ( ) Theft of paperwork or data storage device
- ( ) Social engineering/impersonation
- ( ) Rogue employee/insider threat
- (•) Cyber incident

  A cyber incident targets computer information systems, infrastructures, computer networks, or personal computer devices.

Please provide more detail by selecting one of the following:

- ( ) Malware
- ( ) Brute-force attack (compromised credentials)
- ( ) Ransomware
- ( ) Phishing (compromised credentials)
- ( ) Compromised credentials (method unknown)
- (•) Hacking

  Exploiting a software or security weakness to gain access to asystem or network, other than by way of phishing, brute-forceattack or malware.

- ( ) Other

Number of individuals whose personal information is involved in the data breach

- ○ 1
- ○ 2 – 10
- ○ 11 – 100
- ○ 101 – 1 000
- ◉ 1 001 – 5 000
- ○ 5 001 – 10 000
- ○ 10 001 – 25 000
- ○ 25 001 – 50 000
- ○ 50 001 – 100 000
- ○ 100 001 – 250 000
- ○ 250 001 – 500 000
- ○ 500 001 – 1 000 000
- ○ 1 000 001 – 10 000 000
- ○ 10 000 001 or more

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate:

2000

Number of individuals *in Australia* whose personal information is involved in the data breach

- ○ 1
- ○ 2 – 10
- ○ 11 – 100
- ○ 101 – 1 000
- ◉ 1 001 – 5 000
- ○ 5 001 – 10 000
- ○ 10 001 – 25 000
- ○ 25 001 – 50 000
- ○ 50 001 – 100 000
- ○ 100 001 – 250 000
- ○ 250 001 – 500 000
- ○ 500 001 – 1 000 000
- ○ 1 000 001 – 10 000 000
- ○ 10 000 001 or more

Exact number of individuals *in Australia* whose personal information is involved in the data breach

Please provide your best estimate:

2000

Description of how the data breach occurred

HAFNIUM attack via Exchange server

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach.

No evidence of data taken. Unable to identify any particular individual affected.

Description of any action you have taken, or you are intending to take, to prevent reoccurrence.

All steps to patch against HAFNIUM attack and to remove malicious tools placed on server have been taken.

How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur? If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

Intend to place notification on website, together with this report. Also via social media. Not practicable to notify individuals separately. This is intended to happen the week beginning 27 April 2021.

List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to.

Nil

You may wish to separately report an incident to the Australian Cyber Security Centre if it raises cyber security concerns.

Notification

Please attach a template copy of your notification to affected individuals.

File: None

Additional information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to enquiries@oaic.gov.au.

Attachments

☐ I request that the information provided in part two of this form is held by the OAIC in confidence.

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

Review and submit

Submitting your form

Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the
Go Back button.

Once you are ready to submit your form, click the **Submit** button below.

Once you submit your form, you will be taken to a confirmation page. This page will provide a receipt number for your submission, and you will be able to download a copy of your completed form or have a copy sent to an email address of your choice.