July 2022

Pharmacy Insights

The Privacy Landscape in Australia following the introduction of the Notifiable Data Breaches (NDB) scheme in 2018

The Office of the Australian Information Commissioner (OAIC) introduced the Notifiable Data Breaches scheme in February 2018 (the Scheme). The Scheme serves the dual purpose of enhancing accountability of entities engaging with personal and sensitive information, and arming affected individuals with the necessary information to lessen the severity of a data breach. The Scheme has provided an ongoing point of reference for the state of privacy protection in Australia, through the publication of regular reports by the OAIC. These reports, initially published quarterly and now published twice a year, highlight where and how the data of Australians has been affected by privacy breaches, and allow us to explore if and how the nature of privacy protection and data breaches has changed since the introduction of the Scheme.

How has the privacy landscape in Australia changed over the past four years?

A summary of the data breaches reported since the introduction of the Scheme is set out in the table below:

Notifiable Data Breaches Statistics Report	Number of data breach notifications	Cause of the breaches		
		Malicious or criminal attacks	Human error	System faults
January – March 2018*	63	44%	51%	3%
April - June 2018	242	59%	36%	5%
July – September 2018	245	57%	37%	6%
October – December 2018	262	64%	33%	3%
January – March 2019	215	61%	35%	4%
April – June 2019	245	62%	34%	4%
July - December 2019	537	64%	32%	4%
January – June 2020	518	61%	34%	5%
July – December 2020	539	58%	38%	5%
January – June 2021	446	65%	30%	5%
July – December 2021	464	55%	41%	4%

*As the Scheme commenced on 22 February 2018, data is only available from that date.

The initial OAIC Report for the complete quarter period from April to June 2018 reported 242 breaches.[1] The most recent report, containing statistics for the six month period from July to December 2021, reports 464 notifications.[2] While this may suggest that Australian entities are starting to move towards more secure protection of personal and sensitive information, there are other findings from the OAIC's most recent report which show other trends in the security of Australians' data that warrant exploring.

Which industry sectors have reported the most data breaches throughout the publication of these reports?

The trends from the OAIC reports also allow us to analyse the industry sectors reporting disproportionately high numbers of data breaches. The following table shows a breakdown of the data breaches per sector since the introduction of the Scheme, and shows that the health sector has consistently been the highest reporting sector, responsible for 20% of all breaches in April to June 2018 and 18% of all breaches in July to December 2021.[3] The second-highest reporting sector has consistently been finance, contributing 12% of reported breaches in the latter half of 2021.[4]

Notifiable Data Breaches Statistics Report	Top reporting sectors and % of notifications		
	Health	Finance	Legal, accounting and management services
January – March 2018*	24%	13%	16%
April - June 2018	20%	15%	8%
July – September 2018	18%	14%	14%
October – December 2018	21%	15%	9%
January- March 2019	27%	13%	11%
April – June 2019	19%	17%	10%
July - December 2019	22%	14%	7%
January – June 2020	22%	15%	5%
July – December 2020	23%	15%	7%
January – June 2021	19%	13%	8%
July – December 2021	18%	12%	11%

*As the Scheme commenced on 22 February 2018, data is only available from that date.

The high number of breaches in the health sector is due to the nature and volume of personal information held by health service providers – including sensitive information such as an individual's medical history.

[1] Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 April to 30 June 2018* (Quarterly Report, 2018) 4 (*'2018 OAIC Report'*).
[2] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July–December 2021* (Biannual Report, 2021) 5 (*'2021 OAIC Report'*).
[3] *2018 OAIC Report* (n 1) 13; *2021 OAIC Report* (n 2) 19.
[4] *2021 OAIC Report* (n 2) 19.

How do breaches in the health care sector occur, and has their cause been consistent over time?

The main categories of reported data breaches across the board are malicious or criminal attacks and human error. In particular, the percentage of data breaches attributed to human error over time is not declining. The number of notified breaches across all sectors and attributed to human error was 36% in the April – June 2018 quarter, and had increased to 41% for the six month period in the most recent 2021 report.[5] This statistic reminds us that human error and the role of people in privacy protection cannot be overlooked.

The following table shows a summary of reported breaches in the health sector since the introduction of the Scheme.

Notifiable Data Breaches Statistics Report	Number of notifications in the health sector	Cause of breaches within the health sector		
		Malicious or criminal attacks	Human error	System faults
April - June 2018	49	41%	59%	0%
July – September 2018	45	42%	56%	2%
October – December 2018	54	46%	54%	0%
January – March 2019	58	45%	52%	3%
April – June 2019	47	47%	53%	0%
July - December 2019	117	54%	43%	3%
January – June 2020	115	40%	57%	3%
July – December 2020	123	41%	57%	2%
January – June 2021	85	56%	41%	2%
July – December 2021	83	47%	47%	6%

As the table illustrates, a high proportion of reportable data breaches in the health sector occur due to human error: 59% in the quarter from April and June 2018 and 47% in the six-month period from July to December 2021.[6] While the decrease is comforting, the OAIC reports find that data breaches in the health sector are attributed to a range of human errors, including (but not limited to):

- personal information being sent to the wrong recipient (by email, mail or other)
- unauthorised disclosure of information due to unintended release or publication, or verbal disclosure, and
- loss of paperwork, laptop or data storage device.

While these mistakes may be simple to make and in many cases occur without malice, the consequences can be severe, both for the individual and entity concerned. The most recent 2021 report indicated a new trend for data breaches caused by human error in the health sector as a result of failure to use the BCC function when sending an email. This is where an email is sent to a large mailing list, and the sender fails to use the BCC function, resulting in mass exposure of personal information including names and emails to other recipients.[7]

[5] *2018 OAIC Report* (n 1) 7; *2021 OAIC Report* (n 2) 5.
[6] *2018 OAIC Report* (n 1) 25; *2021 OAIC Report* (n 2) 21.
[7] *2021 OAIC Report* (n 2) 17.

To prevent human errors occurring, it is important to ensure that policies on the handling and storage of personal information are clear and concise, that staff understand and are adequately and frequently trained on their privacy obligations and suspected breaches are notified, investigated and escalated promptly.

What are the reporting responsibilities for organisations with identified data breaches?

When a suspected data breach occurs, as a result of human error or otherwise, it may need to be reported under the Scheme and the individual(s) concerned may also need to be informed that their privacy has been breached.

A breach will be an 'eligible data breach' if it involves:

1. unauthorised access, disclosure or loss of personal information, and
2. a reasonable person would conclude that the breach will result in ***serious harm*** to one or more individuals, and
3. the organisation responsible for the breach cannot take remedial steps to prevent the likelihood of serious harm.

The trends shown in the OAIC reports highlight that privacy protection continues to be a challenge for Australian entities, in particular for organisations operating in the health provider sector. While there may be less notifications now than when the Scheme first commenced four years ago, there continues to be a wide range of causes responsible for these breaches, and human error continues to be a leading contributor. As a result, it is imperative that Australian organisations remain diligent in their protection of privacy, keep abreast of changing privacy practices and trends and continually educate their workforce to work towards a more secure privacy landscape for Australia.

Further Resources

For further information about reporting a data breach, see the OAIC resources available here.
Further information about the data breach statistics published under the Scheme are available here.

This article was written by Special Counsel Hayley Bowman. If you have any questions about how your organisation handles personal or sensitive information, or require assistance in reviewing your privacy practices and policies, please contact Hayley.

Hayley Bowman | Special Counsel
T +61 2 9018 9975
E godell@meridianlawyers.com.au

Disclaimer: This information is current as of July 2022. This article does not constitute legal advice and does not give rise to any solicitor/client relationship between Meridian Lawyers and the reader. Professional legal advice should be sought before acting or relying upon the content of this article.