Freedom of Information (Scotland) Act 2002

Date received	22/08/2022	**Subject**	Data Breaches		
Passed to	Information Governance	**Date passed**	23/08/2022	**Respond by**	12/09/2022
Category	Scottish Parliament	**FOI number**	2022-335		

Question/s to be answered

For clarity, I am defining a data breach as follows:

'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.'

Or:

'As a security incident that has affected the confidentiality, integrity or availability of personal data.'

1. In this health board, how many data breaches have been recorded so far in the 2022 calendar year? Please also provide the data for the 2021, 2020, 2019, 2018 and 2017 calendar years.

Year	Number of incidents	Number reported to ICO
2017	45	N/A
2018	44	2
2019	57	10
2020	70	11
2021	115	7
2022 to 22 August	53	5

Please note the following:

- The figures in the table above only include incidents for which NHS Shetland was the sole or joint data controller. While we do record incidents for which NHS Shetland is not the data controller (for instance, if patient information is erroneously sent to NHS Shetland by another health board / data controller) we have not included these incidents as NHS Shetland has no responsibility for them.

- Since the advent of the GDPR and Data Protection Act 2018 (DPA 2018), NHS Shetland has carried out extensive work in training / raising awareness of data protection issues as well as improvements to the categorisation of data incidents on our adverse event reporting system, leading to an increase in numbers of incidents reported and categorised as data incidents.

- NHS Shetland records and investigates all data breaches reported through our adverse event reporting system, regardless of severity. As part of the investigation process, and in accordance with our duties under the UK-GDPR, we assess whether each incident is likely to result in harm to the rights and freedoms of the data subject(s) involved. If this is assessed to be the case, we self-report the breach to the Information Commissioner's Office (ICO).

  In all the incidents reported to the ICO to date and for which the ICO has issued a decision notice, the ICO has determined that no further action was necessary.

2. In this health board, where a data breach has been recorded in the 2022 calendar year so far, what was the nature of the breach? For example, was patients' private medical information leaked or was personal information released like addresses and phone numbers? Please also provide the data for the 2021, 2020, 2019, 2018 and 2017 calendar years.

   NHS Shetland defines incidents using the categories used by the ICO in their reporting. Using these categories, the breakdown by year is as follows:

   2017

Incident type	**Count**	**Reported to ICO***
Alteration of / error in personal data	25	N/A
Data emailed/texted to the wrong recipient	3	N/A
Data posted/faxed/handed to incorrect recipient	6	N/A
Hardware/software misconfiguration	1	N/A
Loss/theft of paperwork/data or paperwork/data left in unsecure location	5	N/A
Other non-cyber incident	3	N/A
Unauthorised access	1	N/A
Verbal disclosure of personal data	1	N/A
Grand Total	**45**	**N/A**

   *Prior to the introduction of the GDPR and DPA 2018 there was no requirement to report incidents to the ICO.

Freedom of Information (Scotland) Act 2002

2018

Incident type	Count	Reported to ICO
Alteration of / error in personal data	4	0
Data emailed/texted to the wrong recipient	2	0
Data posted/faxed/handed to incorrect recipient	18	0
Hardware/software misconfiguration	5	1
Loss/theft of paperwork/data or paperwork/data left in unsecure location	8	1
Other non-cyber incident	5	0
Unauthorised access	2	0
Grand Total	**44**	**2**

2019

Incident type	Count	Reported to ICO
Alteration of / error in personal data	20	0
Data emailed/texted to the wrong recipient	8	1
Data posted/faxed/handed to incorrect recipient	10	4
Hardware/software misconfiguration	3	1
Loss/theft of device containing personal data	1	0
Loss/theft of paperwork/data or paperwork/data left in unsecure location	9	1
Other non-cyber incident	3	1
Unauthorised access	2	1
Unauthorised access (cyber)	1	1
Grand Total	**57**	**10**

2020

Incident type	Count	Reported to ICO
Alteration of / error in personal data	17	2
Data emailed/texted to the wrong recipient	13	0

Data posted/faxed/handed to incorrect recipient	9	5
Failure to redact	3	3
Failure to use bcc	1	1
Hardware/software misconfiguration	5	0
Loss/theft of paperwork/data or paperwork/data left in unsecure location	5	0
Other non-cyber incident	12	0
Unauthorised access	5	0
Grand Total	**70**	**11**

2021

Incident type	Count	Reported to ICO
Alteration of / error in personal data	62	0
Data emailed/texted to the wrong recipient	22	0
Data posted/faxed/handed to incorrect recipient	12	4
Hardware/software misconfiguration	6	1
Loss/theft of paperwork/data or paperwork/data left in unsecure location	4	1
Other non-cyber incident	5	0
Unauthorised access	3	1
Verbal disclosure of personal data	1	0
Grand Total	**115**	

2022 to 22 August

Incident type	Count	Reported to ICO
Alteration of / error in personal data	25	1
Data emailed/texted to the wrong recipient	10	0
Data posted/faxed/handed to incorrect recipient	8	2
Hardware/software misconfiguration	4	1
Other non-cyber incident	2	0

Ransomware	1	1
Unauthorised access	2	0
Verbal disclosure of personal data	1	0
Grand Total	**53**	**5**

3. In this health board, where a data breach has been recorded in the 2022 calendar year, what was the consequence of the breach? For example, was it possible to identify subsequent evidence of malicious use, selling data, or harm to patients? Please also provide the data for the 2021, 2020, 2019, 2018 and 2017 calendar years.

   As noted above, it is only incidents in which there is harm / a likely risk of harm to the data subject that are reported to the ICO. In all other reported incidents there was no (or negligible) risk of harm. For this reason we have only considered ICO-reported incidents for this question.

   For all of the incidents in the time period for which investigations have been completed, no significant harm or other adverse consequences have been reported.

   Under UK-GDPR article 33(1), reporting to the ICO is required when it is likely that there is a risk to the rights and freedoms of the data subject(s). Given the statutory 72-hour window for submitting a report, it is often the case that NHS Shetland will submit a report **before** it is able to confirm whether **actual** harm has occurred, and it is also often the case that subsequent investigations establish that no harm has resulted.

   This practice of submitting initial reports before all information about an incident is known is in line with the guidance provided by the ICO.