

Summary of Information Governance Key Indicators – January to March 2025

SAR Activity

NHSWI received 63 Subject Access Requests in the first quarter of 2025. This annual increase has continued year on year, with the 2025 projected number being around 250 based on the average received in the year to date.

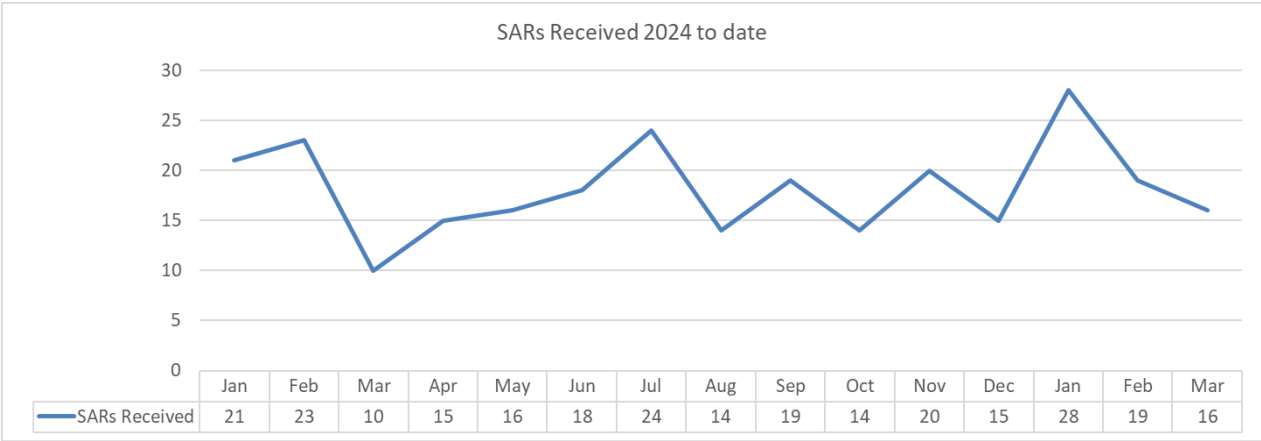
Around a third of requests are for partial records with two thirds typically requesting copies of the full medical record.

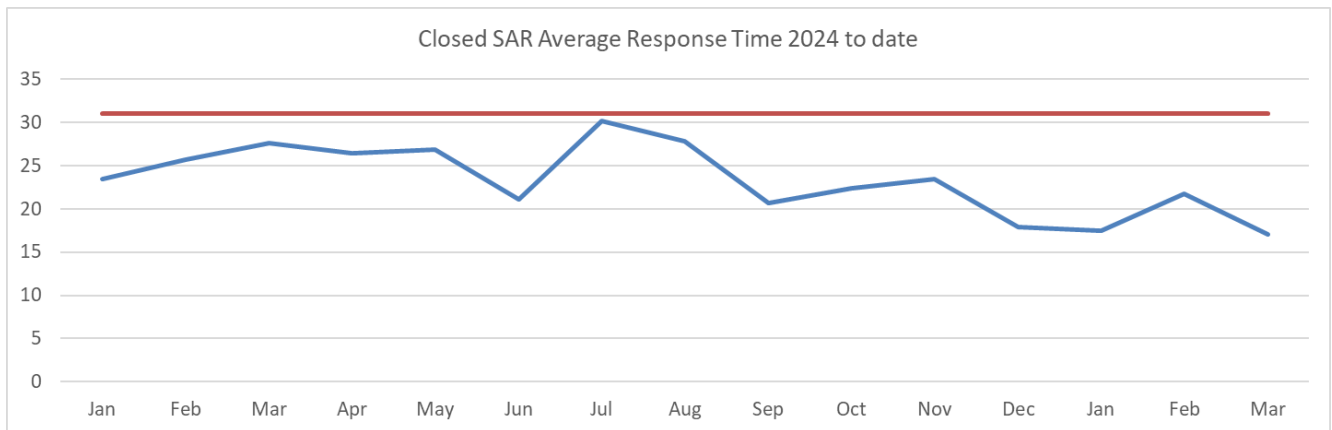


Of the 41 SARs received in 2025 which are closed, overall, around 76% were released within the timescale, breakdown by request type below.

Request Type	Over	Under	Grand Total
2025			
Court	4	2	6
Police	2	4	6
Standard	4	24	28
Standard - GP		1	1
Grand Total	10	31	41

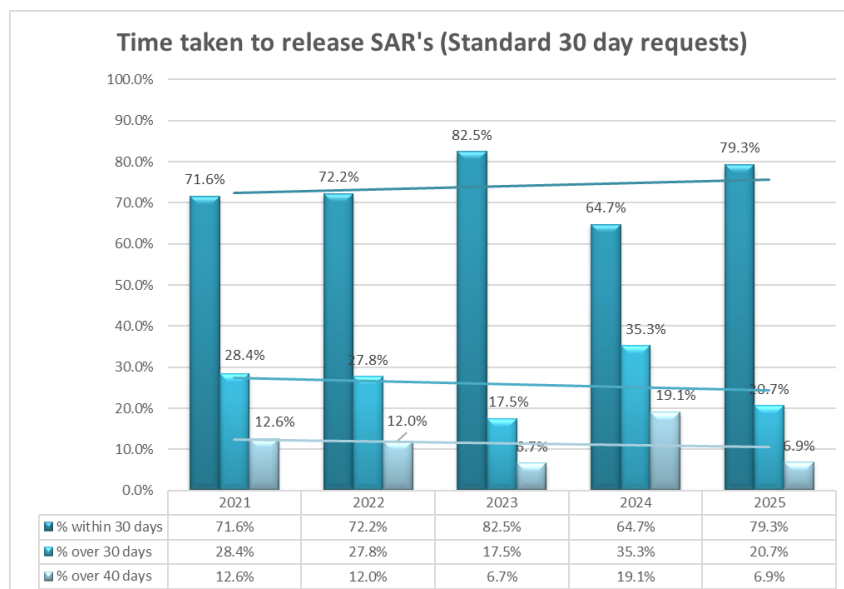
The chart below shows the number of subject access requests received each month, from 2024 to date:





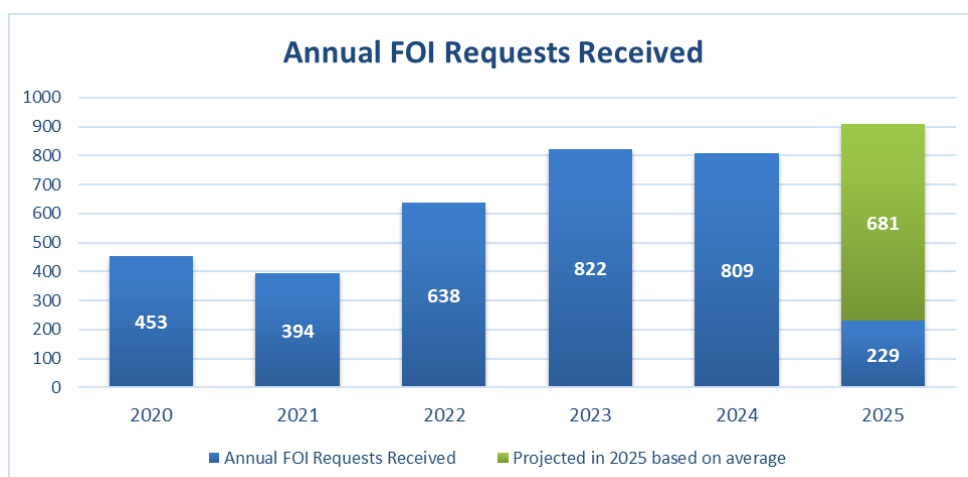
Although, on average for all SARs received, the one calendar month deadline is being met (see above), this includes Police and Court requests that have a shorter deadline.

In 2024, the proportion waiting over 30 days and over 40 days increased. In 2025 for quarter 1, 20% of closed requests were closed after the deadline date.

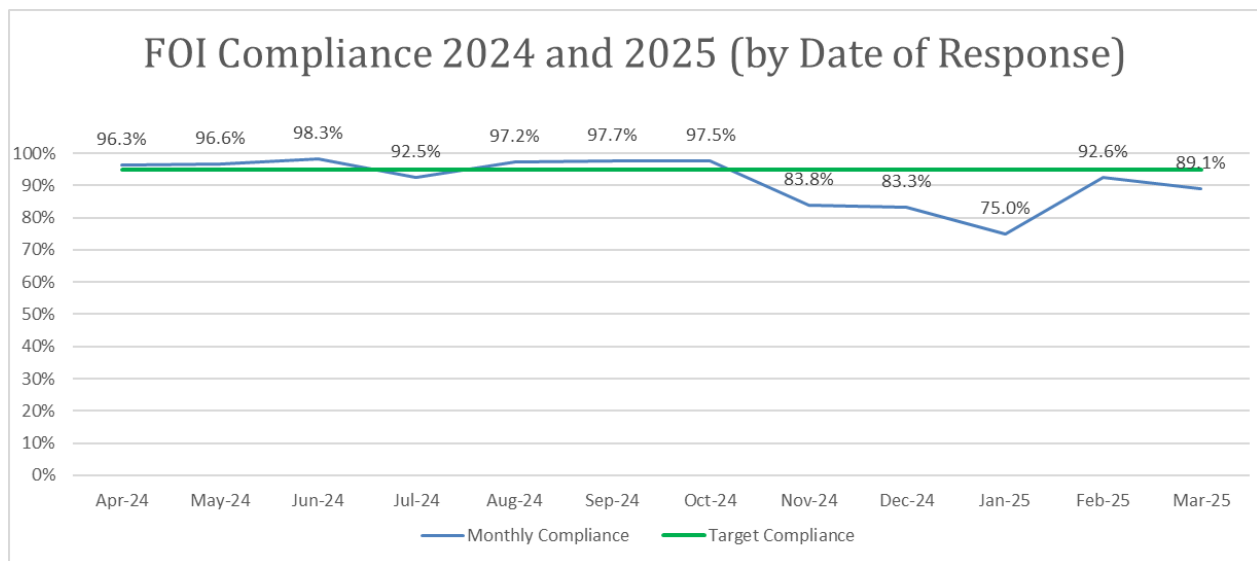


## **FOI Activity**

229 FOIs were received in the first quarter of this year. The end of year projection would be over 900 if these numbers continue.



FOI compliance for Quarter 1 2025 (for all those closed to 31/03/2025) was around 85%, with 32 in the year to date responded to over the 20-working day target.



At the time of this report, there were 37 FOIs still open.

The compliance rate reported to the ICO (by date received) will change as each FOI is closed off in turn, but it's expected that it will be between 80% and 85% for the first quarter of 2025.

In terms of ICO reporting periods, January - March is their Q4 which is not yet published. Below is a summary of NHSWI submissions from January 2023 to December 2024.

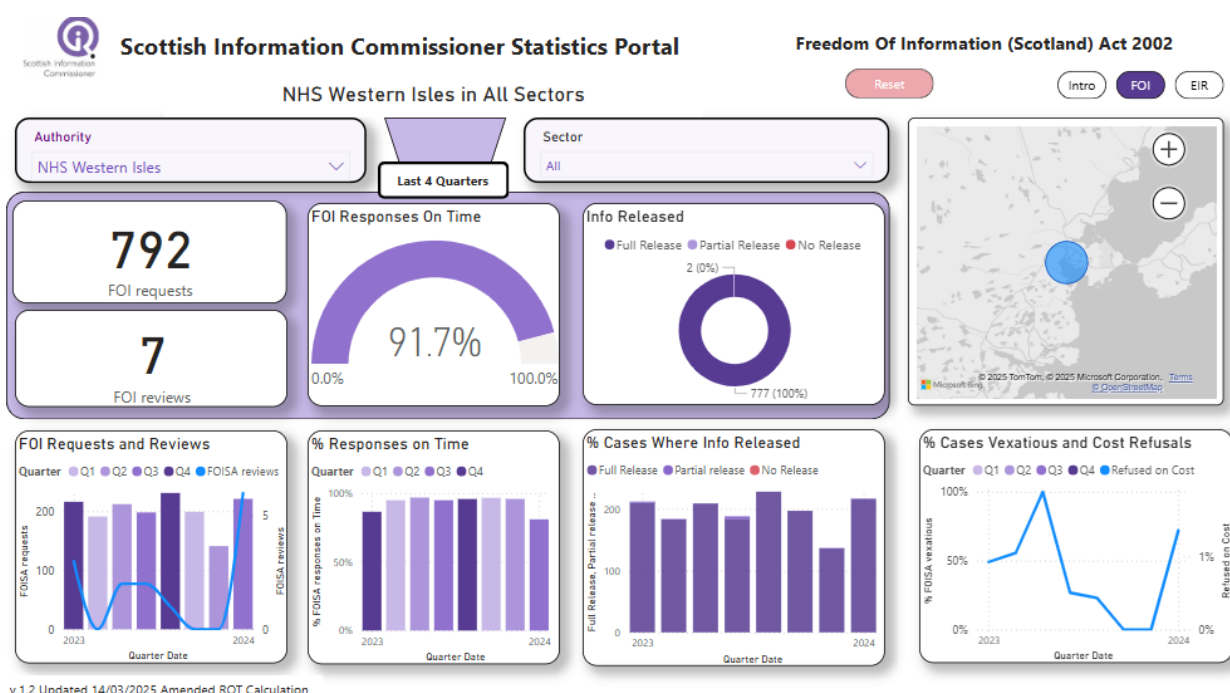
Overall % compliance in the 2-year period – 91%

Q2 2024 – 96%

Q3 2024 – 96%

Q4 2024 – 81%

Q1 2025 – submission date end April 2025



Below is a breakdown of the FOI requests received in 2025, by broad category of request:

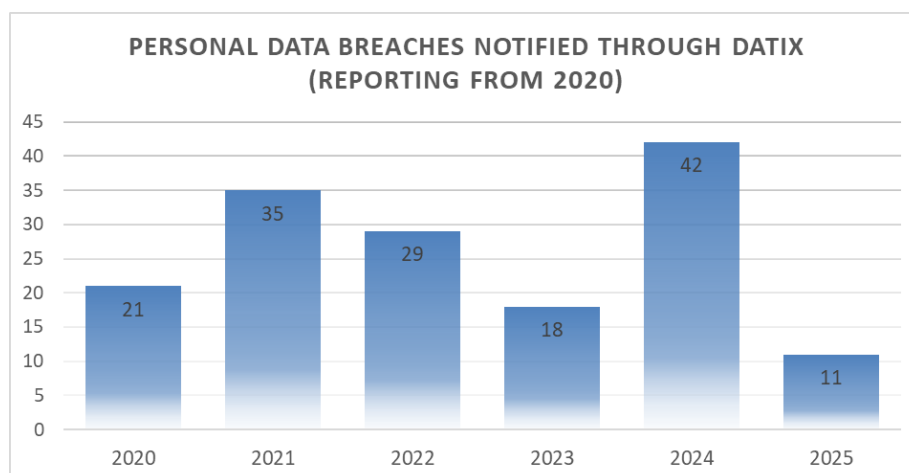
FOI Category	2025
A&E	9
AHP Services	8
Alcohol & Drugs	1
Board	18
Cancer	5
Children	2
Clinical Protocols	3
Clinical Services	46
Delayed Discharges	1
Dental	3
EIR	5
Equipment	5
Finance	30
GP	5
H&S	1
HR	21
Infection Control	1
IT/Contracts	12
Labs	5
Maternity	10
Medication	12
Mental Health	14
Other	2
Radiology	2
Violence & Aggression	2
Waiting Times	6

### **Personal Data Breaches:**

Staff continue to report any actual or suspected data breaches on Datix. This enables us to target training sessions and materials to any areas with a higher rate of incident and put in place steps to mitigate and prevent future breaches.

These include all breaches reported by staff on Datix, including suspected or potential data breaches and, on investigation, may not all have resulted in a data breach. Some staff may have reported the same breach so there may be double counting. Increases in reporting should not always be seen negatively, rather the increase in staff awareness of their responsibility to report and what to look out for.

42 Personal data breaches (or suspected data breaches) Were reported in 2024, and 11 in 2025 to date:



Breach category	2025
Unauthorised Disclosure of Personal Information - Email	3
Unauthorised Disclosure of Personal Information - Other	3
Personal Information found in unauthorised area by Staff	2
Malware Attack - Device Infected containing Personal Information	1
Other - please specify in description	1
Unauthorised Disclosure of Personal Information - Internal Mail	1
Grand Total	11

### **IG Training - Mandatory Learning**

With the move from Learn Pro now complete, three mandatory training modules are all available on TURAS for all staff to take.

A poster was created and was advertised Team Briefs to encourage staff to log on and complete these modules. Two additional modules are now available for staff to take - 'Information Risk Management for Asset Owners' and for 'Data Sharing in Crisis'. These can be taken by anyone but will be targeted at specific staff identified as information asset owners.

Compliance for Safe Information Handling is now at 60%, and monthly reports are being run with emails sent to Department Heads and users to try to increase uptake across all areas.

