Royal Cornwall Hospitals NHS Trust

Staff Data Breach Investigation Report

PSII 255748

Important note

This report is addressed to and for the benefit of Royal Cornwall Hospitals NHS Trust (the Trust) and was prepared for the purpose set out in the terms of engagement agreed between the Trust and Capsticks.

No other person or organisation may rely on this report, and it must not be reproduced in whole or in part without first consulting the authors. Capsticks accepts no duty of care to any other person or organisation.

This report and any accompanying appendices or documents contain confidential information that has not been redacted and may be legally privileged. Care should be taken to ensure that material not intended for wider disclosure is not shared in error. The interviews and legal advice are privileged and are not included with the report.

1. Executive summary

1.1. This report examines the inadvertent disclosure of staff sickness absence data by Royal Cornwall Hospitals NHS Trust in response to a Freedom of Information (FOI) request. In February 2023, the Trust published an Excel spreadsheet as part of its FOI response and disclosure log. Although the visible spreadsheet appeared to contain only aggregate information, interacting with certain cells revealed underlying pivot table data showing line-by-line sickness absence records for April 2018 to January 2023 (with predicted absences extending up to May 2023). This included reasons for absence and duration or dates for named, or potentially identifiable, staff. Some reasons were highly sensitive. In other cases, the material exposed contained entirely typical reasons for sickness. However, all employee health information should be treated as confidential. This data should not have been included. Although the disclosure was accidental, the system of work did not prevent it. The hidden data included names and workplace information for 7,715 current and former Trust staff, similar information for 288 non-Trust workers, and a small number of unmatched records. No financial, banking, national insurance, address or contact information was disclosed.

Summary of key findings

1.2. The incident arose from process failures and system weaknesses in handling the FOI response. Although the Trust had an FOI process in place:

- The spreadsheet was prepared outside the team with the greatest expertise in handling complex workforce datasets, with a long chain of people involved in the creation and review of the material prior to its disclosure.
- The controls in the FOI response process at the time did not effectively address pivot table risks. In particular, the Trust's reliance on Excel's document inspection tools at that time was insufficient, because those tools would not themselves remove the hidden pivot table data or explicitly flag that personal information was hidden in the spreadsheet.

- The Trust's requirement to convert Excel disclosures to PDF before publication was not followed. The incident therefore resulted from weaknesses across the FOI process, from data extraction and preparation to checking, sign-off and publication, rather than a single failure.

Summary of areas for improvement and safety actions

1.3. Since the original file was disclosed in response to the FOI request in 2023, the Trust has made significant changes to the FOI process. Additional safeguards now reflect much of the Information Commissioner's current good practice guidance for public bodies on managing disclosure risks in FOI responses. These safeguards still rely on people, but if applied carefully, consistently and with a second check, they should reduce the risk of similar incidents in future, at least in the FOI context. We recommend that the Trust incorporates the Information Commissioner's Office's other tools and good practice guidance into its processes.

1.4. However, FOI responses are just one way in which incidents of this kind may occur. As organisations process and share increasingly large volumes of data, similar incidents may occur in other contexts. We recommend that the Trust considers:

(1) Rolling out some of the safeguards now in place for FOI requests more widely, for other kinds of disclosures/information sharing exercises it undertakes.

(2) Widening training on digital literacy, particularly for staff in roles using pivot tables.

(3) Considering whether there are reliable electronic tools which could provide additional safeguards to supplement human checks on data and documents prior to sharing. However, the selection of any such tools must not interfere with the legitimate disclosure and sharing of information by the Trust which is vital for patient care and the efficient work of the Trust more generally.

1.5. The Trust identified the incident in November 2025 after a member of the public alerted it to the material on the Trust's website. The Trust promptly removed the material, reported the breach externally, and launched an extensive internal response. This included notifying current and former staff, setting up a dedicated contact centre, holding staff briefing sessions, and reviewing historic disclosures. The FOI response process was immediately strengthened with additional safeguards to prevent similar spreadsheet disclosures. This was the first incident of its kind in terms of the scale and severity, and accordingly, the Trust's response was necessarily evolutionary. There are lessons from the way this incident occurred which were unknowable during the incident itself and have become apparent only with reflection. The investigation considers that the Trust acted promptly and in good faith once the incident came to light and met its reporting obligations overall. The Information Commissioner closed its case after the Trust's self-report and issued advice, which appears to have been fully implemented. The investigation identified lessons on preparedness, staff support, consistency of communications, and ensuring adequate resources for any future incident of this kind. The Trust could also, if it wished, make a further attempt through other channels to ask the original FOI requester to delete the information.

1.6. The scale and sensitivity of the data exposed had significant consequences for affected individuals and for the Trust. The response was resource-intensive and placed substantial pressure on those managing it. Some staff were left deeply upset, reported a loss of trust in the organisation, and remained concerned about possible misuse of their personal information, especially where the data related to sensitive health conditions or personal circumstances. However, the investigators found no evidence that the data has in fact been misused.

1.7. The report concludes that the Trust should continue to strengthen both its technical and organisational controls for disclosing information, particularly where spreadsheets or large datasets are involved. Key recommendations in this area include:

(1) Ensuring that the FOI response process is updated to require that data files be converted to CSV wherever possible before disclosure.

(2) Embedding clearer guidance on pivot tables and hidden data risks into FOI procedures (particularly for 'information holders') – although this recommendation is applicable for any such disclosures.

(3) Maintaining the second-stage review of disclosure material.

(4) Clearer delineation of responsibilities between information-holding teams and the FOI function in the Information Governance (IG) team.

(5) To increase use of SharePoint or other file sharing mechanisms (rather than emails) which allow for access to data to be 'turned off' if it is disclosed in error, and to explore other technical data loss prevention tools; and

(6) Widening role-specific training on data handling across the organisation (not limited to the FOI context, but for all staff who are routinely involved in data analytics where large pots of data may be shared externally or with large audiences in their work).

1.8. The Trust should also capture the operational and strategic lessons from the extensive incident response, including by ensuring that in future cases:

(1) There is an appropriate level of support and resources for staff managing high-volume contact operations.

(2) There are effective deputization and knowledge sharing arrangements so that the Trust is not over-reliant on single members of staff to coordinate or deliver key steps in incident responses.

(3) The data breach process is integrated into the Emergency Planning and Resilience Response (EPRR) processes more generally and incident planning factors in data loss events as well as cyber-attacks (or other recall or large-scale staff/patient contact exercises).

(4) future engagement exercises with affected individuals in any incident continue to be timely, consistent and trauma informed.

1.9. Taken together, these actions will reduce the risk of recurrence and improve the Trust's resilience should a similar incident arise in future.

1.10. The Trust should continue to de-brief with the affected teams that were involved in the incident and the response.

1.11. We finish this executive summary with a note of sincere thanks to all the staff that contributed to this investigation. Everyone did so voluntarily, openly, honestly and frankly, and in line with the Trust's values, through participating in interviews or by providing documentation and other resources in a timely manner, or by taking the time to provide survey responses. The independent investigation team at Capsticks would like to highlight the work of Naomi Burden who has provided outstanding support and assistance throughout.

Table of Contents

1. Executive summary 3
2. Background and context 10
Overview 10
The Freedom of Information Act 2000 11
Freedom of Information requests: general principles 11
Specific ICO guidance on avoiding disclosure in error in response to FOI requests 13
Description of the Incident 17
Who was affected? 26
3. Investigation approach and terms of reference 28
The Investigation Team 28
Scope and Terms of Reference 28
Scope 28
Terms of reference 29
Part 1: Events leading and contributing to the incident. 29
Part 2: Learning and Improvement 29
Summary of investigation process 30
Information gathering 31
4. Findings: The Initial Incident 32
The FOI Request 32
People Factors 32
Systems of Work 34
Governance and handling of FOI requests at the Trust 34
Organisational factor: Information Governance Team structure 34
Organisational factor: Information Use Framework Policy 36
Task Factor: FOI Standard Operating Procedures 36
Tools and Technology Factor: Use of digital technology 39
Task factor: Freedom of Information Guidance for Information Holders 42
System Weaknesses: Key Contributory Factors (CFs) 43
CF1: Allocation of 'Information Holder' staff responsible 43
CF 2: Creation of the spreadsheet 46
CF3: Processing of the FOI request by the Information Governance team 47

CF4: Approval / Sign off 49
Training and supervision of FOI officers 50
5. Changes to information governance arrangements for publishing FOI responses since the breach 53
6. Findings: Responding to the incident and Incident management 56
The personal impact of the data breach 56
Context: morale among some staff affected by the incident 59
Timeline of incident response 59
Regulatory reporting obligations and consequences 62
What lessons can be learned from the way the incident was handled? 64
Incident response team 64
Review of previous FOI responses 65
Brief of external support 65
The Trust wrote to approximately 5000 current staff and 3000 former staff to tell them about and apologise for the error 65
The PIU Lead undertook extensive data analysis to support the incident response. 67
Creation of a guide for staff to find their information 70
MS Teams Live question and answer sessions with staff 71
Email address for queries 74
The Contact Call Centre 74
E-Rostering improvements 81
Investigation staff survey 82
Summary of findings, areas for improvement and safety actions 85
References 89

2. Background and context

Overview

2.1. The safe handling and security of information in the UK is governed by regulations and legislation that are used to define local systems of work. Organisations must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and 'common law' duties of confidentiality when processing both patient and staff data. The Information Commissioner's Office is the independent regulatory body responsible for upholding information rights. It enforces data protection legislation as well as the Freedom of Information Act 2000 (FOIA).

2.2. Staff information is held in relation to employment and includes personal sensitive information that is legitimately collected, such as contact details, financial information and health information.

2.3. Within the legal framework provided for, workers would expect health information to be handled carefully and not used in ways that have an unjustified adverse effect on them. This therefore necessitates clear working processes for processing health information internally through policies and restricting access. The Royal Cornwall Hospitals NHS Trust, like all organisations, must ensure appropriate information governance arrangements, including:

- Maintaining an Information Security Management System (ISMS) to monitor and improve data security practices.
- Annual completion of the Data Security and Protection Toolkit (DSPT), demonstrating compliance with national data security standards.
- Management of FOI requests through designated Information Governance teams to ensure compliance, appropriate redaction, and secure handling of information.

2.4. The FOIA provides a statutory right of access to recorded information held by public authorities, including NHS Trusts. It promotes transparency and accountability, with disclosure as the default unless a lawful exemption applies.

2.5. Key principles include:

- Right of access: Anyone can request information, regardless of identity or motive.
- Timeliness: Responses must be provided within 20 working days.
- Duty to assist: Organisations must help clarify requests where needed.
- Recorded information only: There is no requirement to create new information.

2.6. FOI disclosures are effectively public releases and must be considered suitable for wider publication. There are exemptions that can be applied and a formal refusal notice issued.

The Freedom of Information Act 2000

Freedom of Information requests: general principles

2.7. NHS Trusts are public authorities under the FOIA. FOIA gives any person a statutory right to request recorded information held by a public body (i.e. make an FOI Request). It is intended to promote openness, transparency and accountability across the public sector, including the NHS. The Trust has 20 working days to respond.

2.8. The general principle with FOIA is that the Trust should take an ‘applicant and motive blind’ approach in responding to FOI requests. However, the Trust is aware that in the context of this specific case, the original FOI applicant used a Gmail account which appears likely to have been created as a ‘burner’ account, solely

for use to make FOI requests relating to absences from stress for the purposes of producing an article regarding the same. Disclosure under FOIA is 'to the world' and in the terms of FOIA itself, the Trust does not have any control over how the FOIA response, including any information disclosed within it, may be used by the person to whom it is disclosed. This means there is no practical or legal control over how such material is used. Although there is a framework to impose licence conditions on material disclosed under FOIA in response to requests for reuse by members of the public under the Reuse of Public Sector Information Regulations 2015, this specifically excludes the reuse of personal data.

2.9. Online searches suggest the FOI request at the heart of this incident formed part of a 'round robin' sent to multiple NHS organisations. Gloucester Health & Care NHS Trust, South East Coast Ambulance Service, and Birmingham and Solihull Mental Health NHS Trust each published responses to similar requests on their websites.

2.10. Section 11 FOIA requires the Trust to respond to a request *"by communicating information by any means which are reasonable in the circumstances"*. In deciding what is reasonable, the Trust may take into account the form in which it holds the information, the volume of information to be communicated and any other relevant factor. There is no absolute duty on the Trust to disclose the information in a particular format, in response to a request. It is required to do so only *"so far as reasonably practicable to give effect to that preference".* Questions of information security may be a relevant consideration in determining what is reasonable. Good practice under FOIA is that information is presented in a re-usable format. Where the information is from or constitutes a dataset (and arguably, the information requested here is that), there is a particular obligation to consider presenting it in a reusable format. The ICO's current (undated) guidance on this issue (https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/means-of-communicating-information-section-11/) states:

> *"When providing information in a re-usable format, you should take steps to ensure that any exempt information in the underlying data is redacted to avoid inadvertent disclosure. For example, you should ensure that any personal data is redacted so it is not unintentionally disclosed. The risk of this happening occurs with spreadsheets in particular. Therefore, you should ensure that requested information is prepared safely for release. For example, when data is presented in the form of a 'pivot' table, the source data is retained. If possible, you should consider disclosing the information in a CSV file format instead. "*[1]

2.11. It is important to recognise that Personal Data (that is, information about a living person who is identifiable from that information or other information which would render them identifiable) is potentially exempt from disclosure under section 40(2) FOIA. There is no absolute prohibition on the disclosure of personal data in response to FOI requests – the legal test is whether it is fair, lawful and necessary to disclose that personal data in response to an FOI request. However, in the case of 'special category' (sensitive) personal data (including information about a person's health), this is highly likely to be exempt from disclosure under FOIA. It is important to recognise that had the original request been for personal data, this would have been exempt from disclosure and the FOI request would not have been progressed.

Specific ICO guidance on avoiding disclosure in error in response to FOI requests

2.12. The disclosure of sensitive information in error in FOI responses is a common problem across the public sector and has been for many years, and a large number of incidents have been publicly reported involving both the NHS and other public sector bodies. There is an underlying tension between FOI law (which requires information to be disclosed promptly by public authorities in response to requests, insofar as possible without restriction on how the data may be used) and

[1] See also, section 11 FOIA.

requirements under confidentiality and data protection law (which say that information must be protected from accidental or unauthorised disclosure or use). This tension has been made more complex as organisations increasingly digitise their systems and processes, which enable large amounts of data to be contained within a single database, typically with the facility to export that data in a format which in turn allows it to be requested and disclosed under FOIA. As a result of this there is a significant inherent risk that the 'wrong' information may be disclosed in error in response to an FOI request.

2.13. In consequence of the recurrent nature of this problem, the Information Commissioner's Office ("**ICO**", which regulates FOIA and data protection issues) has published various pieces of guidance specifically concerning the importance of removing 'hidden' personal data when disclosing information. The first version of this was originally published in 2015, with significant updates in 2018 post-GDPR. The guidance from that time remains publicly available at: https://ico.org.uk/media2/j2wpmnw2/ic-415122-c5k2-disclosure.pdf.

2.14. This is the guidance that would have been in place at the time of the incident which is the subject of this investigation. The guidance is not legally binding. It was (in the ICO's view) supposed to provide a practical "how-to" document aimed at preventing accidental disclosure of personal data when organisations release information in response to FOI/EIR requests (as here), as well as other kinds of request such as subject access requests and disclosures for re-use of public sector information. It focuses on the ways personal data can remain embedded in files even when it appears removed, particularly through hidden data risks in spreadsheets (e.g. hidden rows/columns, additional worksheets, pivot tables, charts and functions) most specifically in paragraphs 33-48. As regards pivot tables, it says:

Copy the pivot table and paste only the values to a new workbook. This is sometimes referred to as a 'paste special' operation. The copied data can also be checked by double-clicking cells within the copied pivot table to ensure there is no link back to the source data. However, exporting the data to CSV would provide a greater assurance and provide greater compatibility with other software packages.

2.15. The ICO guidance in force at the time also included as an appendix structured checklist intended to be used as prompts for repeatable pre-disclosure control (referencing Pivot Tables), although this does not contain any information about action to take in response.

2.16. We analyse in paragraph 4.15 below the extent to which the Trust's systems and processes in place at the time of the incident were compatible with that guidance.

2.17. In the summer of 2023, and then in 2025, following a series of national incidents, the ICO issued updated guidance on this risk (respectively, their guidance can be found at https://ico.org.uk/for-organisations/eir-and-access-to-information/information-commissioner-s-office-advisory-note-to-public-authorities/ and https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/disclosing-documents-to-the-public-securely/). The updated ICO guidance focuses on redaction techniques, avoiding hidden data, and secure handling for FOI and Subject Access Requests. The guidance contains various recommended steps to help check documents for hidden personal information and to remove or redact it, where appropriate. It also contains guidance and links to help organisations consider an appropriate format for disclosure and 'how to' videos and checklists to support the development of policies, procedures and training.

2.18. This ICO guidance does not specify a single method as to how material should be removed, but rather emphasises the need for effective controls. It points out that password protection is a method that can be used to protect documents, but that it can be prone to error, and therefore removal of sensitive material (instead of just making it technically difficult to access) is also an important consideration. The guidance does include that converting spreadsheets into a simpler file format (e.g. CSV) can expose previously hidden information.

2.19. In November 2023, the ICO further published a non-mandatory good practice 'checklist' tool for disclosures of datasets in Excel files. This resource is not well-signposted on the ICO's website, but provides a more practical reference point for issues to look out for with spreadsheets to avoid inadvertent disclosure, see https://ico.org.uk/media2/for-organisations/documents/4026755/disclosure-checklist-v1_0.docx . It is strongly recommended that this guidance is incorporated into the Trust's process as a way of tracking that checks have been undertaken on files prior to disclosure.

2.20. There is also national government guidance regarding the issue of wrongful disclosure in response to FOI requests, updated in December 2023 (and therefore also post-dating the incident). This is not designed for the NHS but contains general useful tips: https://www.gov.uk/government/publications/cabinet-office-and-freedom-of-information/freedom-of-information-guidance-communication-by-spreadsheet . As best the investigators are aware, there is no NHS-wide, specific/practical guidance on avoiding accidental disclosures. The Trust could, as part of learning from this incident, contact NHS England to see what interest there is in providing national guidance on this issue, given that the incident under consideration is not unique to the Trust.

Description of the Incident

2.21. On 18 January 2023, the Trust received an FOI request related to staff sickness information. The wording of the request was as follows:

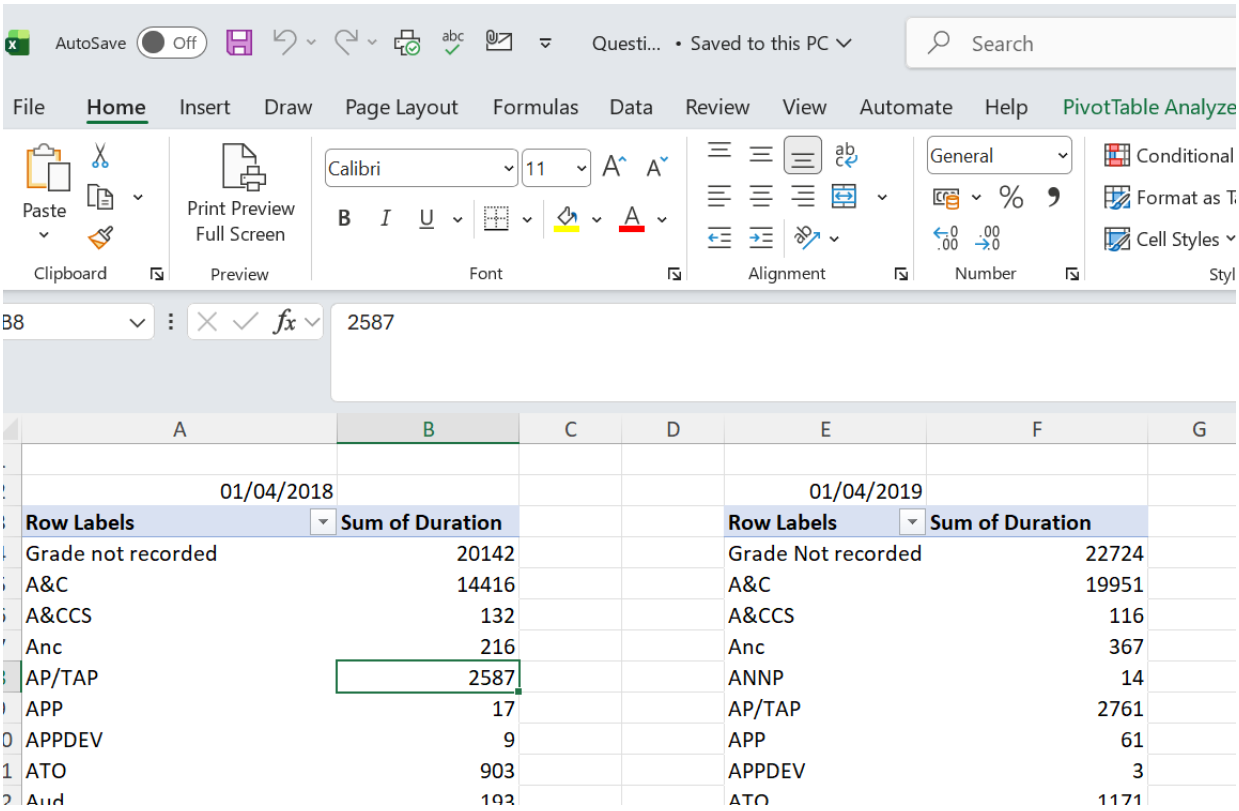
> *For each financial year (i.e. (a) 2022/23, (b) 2021/22, (c) 2020/21, (d) 2019/20, (e) 2018/19):*
>
> *1) How many days have trust staff taken off (sick leave not holiday)?*
>
> *2) How many days have trust staff taken off for stress or anxiety?*
>
> *3) Please provide a staff breakdown for the figure for question two – i.e., how many days were taken off by doctors, nurses, porters, cleaners, admin staff etc.*
>
> *4) How many days have trust employees taken off due to (a) covid and (b) Covid contact-related self-isolation?*
>
> *5) How many trust staff have taken more than a month off in one given year due to stress or anxiety.*
>
> *6) What was the longest period a single member of staff has taken due to stress or anxiety? Please provide their job type or role if possible and an answer for each year.*

2.22. The Trust operates a 'hub and spoke' model for handling FOI requests, which is common in NHS organisations and many other public sector bodies. In this model, a central team is responsible for coordinating the overall response to the FOI request on behalf of the organisation. The central team will contact relevant departments which may hold or be able to access the information in the request (typically via a designated 'champion' member of staff or single point of access). The department will collate the information from systems, databases or other information sources available to them (and/or advise if it considers any information which is within the request is exempt, etc.), and then return it to the central FOI management team, who will then produce and send the final response to the FOI applicant. That is broadly what happened in this case, although as described below, there were a number of departures from the Trust's FOI standard operating procedure (SOP) in the handling of this request which the investigators consider are significant factors in the incident occurring.

2.23. The Trust responded to the applicant via email on 1 February 2023 (and therefore within the 20-working day statutory deadline required by FOIA). The FOI response was also posted onto the Trust's public facing website within the 'FOI disclosure log' page in February 2023. The response provided aggregate information within a letter for questions 1-2 and 4-6, and attached an ostensibly single page Excel spreadsheet which provided the breakdown requested in question 3. This spreadsheet had been generated from within an HR system holding the information within the Trust.

2.24. Unfortunately, the Excel spreadsheet in question used to provide the response to question 3, and included with the response, contained a pivot table feature which included an extract from the HR system's underlying data about staff sickness within it.

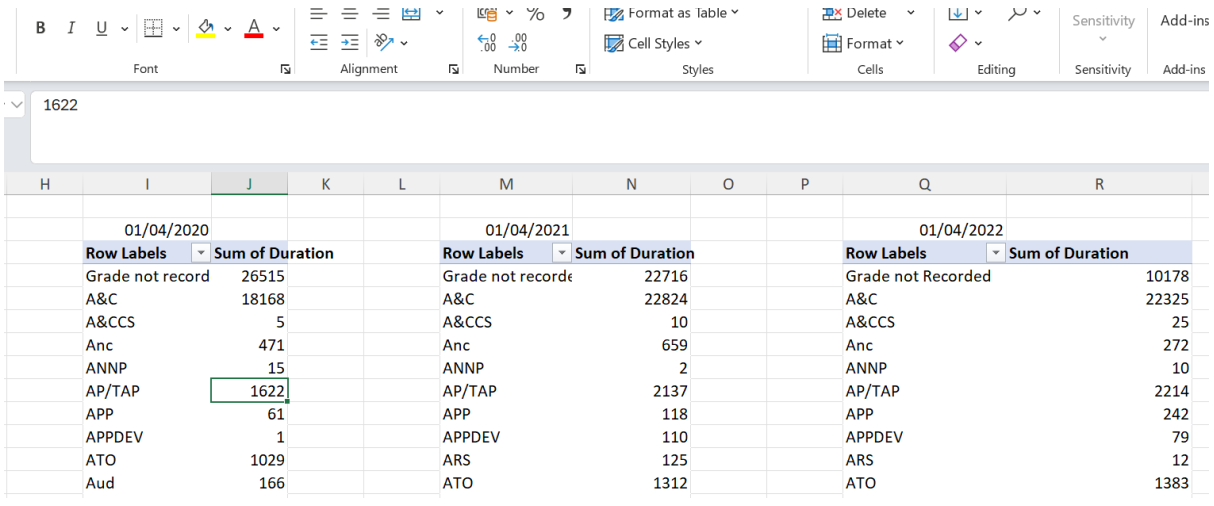
2.25. The baseline format of the spreadsheet on opening it is shown in the screenshots below:



Row Labels	Sum of Duration
Grade not recorded	20142
A&C	14416
A&CCS	132
Anc	216
AP/TAP	2587
APP	17
APPDEV	9
ATO	903
Aud	193

Row Labels	Sum of Duration
Grade Not recorded	22724
A&C	19951
A&CCS	116
Anc	367
ANNP	14
AP/TAP	2761
APP	61
APPDEV	3
ATO	1171

Figure 1 - Screenshot (1) of the spreadsheet disclosed (left hand columns)



Row Labels	Sum of Duration
Grade not record	26515
A&C	18168
A&CCS	5
Anc	471
ANNP	15
AP/TAP	1622
APP	61
APPDEV	1
ATO	1029
Aud	166

Row Labels	Sum of Duration
Grade not recorde	22716
A&C	22824
A&CCS	10
Anc	659
ANNP	2
AP/TAP	2137
APP	118
APPDEV	110
ARS	125
ATO	1312

Row Labels	Sum of Duration
Grade not Recorded	10178
A&C	22325
A&CCS	25
Anc	272
ANNP	10
AP/TAP	2214
APP	242
APPDEV	79
ARS	12
ATO	1383

Figure 2 – Screenshot (2) from spreadsheet disclosed (right hand columns)

2.26. However, the data in the *'Sum of Duration'* columns in Excel spreadsheet were drawn from pivot tables. This meant if you double-clicked on any of the numerical value cells in the 2020, 2021 and 2022 *"Sum of Duration*" column (e.g. any cell in the column containing the one highlighted in

2.27. Figure 2), hidden tabs would then open. These comprised "spreadsheets within a spreadsheet", showing detailed individual absence records. The data fields within these hidden spreadsheets comprised:

a) Surname.

b) Unit.

c) Forename.

d) Grade (or Grade Type and Category).

e) Job Band.

f) Reason for absence (e.g. Covid +, Infectious disease, stress/anxiety etc.).

g) Start date (i.e. of sickness).

h) End Date (i.e. of sickness).

i) Duration (i.e. of sickness).

(i) Working Days.

(ii) Hours.

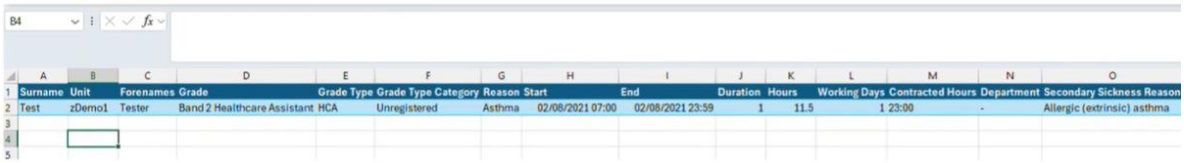
j) Contract Hours.

k) Department.

l) Secondary Sickness reason.

2.28. It is important to note that **no** financial, bank account, national insurance number, address, dates of birth or contact information was included in the spreadsheet and this therefore did not feature in the incident.

2.29. An example of the presentation of the data fields and format is shown in Figure 3 below.

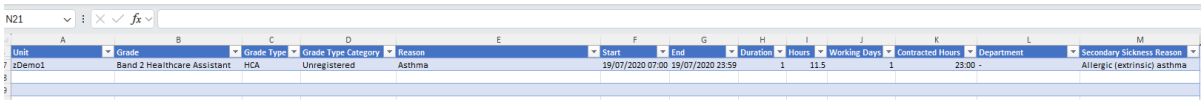


Surname	Unit	Forenames	Grade	Grade Type	Grade Type Category	Reason	Start	End	Duration	Hours	Working Days	Contracted Hours	Department	Secondary Sickness Reason
Test	zDemo1	Tester	Band 2 Healthcare Assistant	HCA	Unregistered	Asthma	02/08/2021 07:00	02/08/2021 23:59	1	11.5	1	23:00	-	Allergic (extrinsic) asthma

Figure 3 - Example of Information Disclosed for 2020, 2021 and 2022 (as shown in Data Breach Information and Q&A sessions)

2.30. If a numerical cell in the 2018 and 2019 *"Sum of Duration"* columns (e.g. the cell showing 2587 in Figure 1 above) was clicked on, a hidden tab would also open. This includes similar data fields to the 2020-2022 fields. However, the individual absence records for these years did not include the names of the staff members concerned. This would be regarded in data protection law terms as likely to constitute 'pseudonymised' data – there is still enough information included in the spreadsheet for (e.g.) a member of staff with knowledge of the department to triangulate and to deduce, or at least make an educated guess, of who the staff member concerned is, and therefore why they were off sick, although it is harder to work out. In some cases, no specific individual may be identifiable, in which case the information is 'anonymised'.

2.31. An example of the data fields for 2018 and 2019 is shown in Figure 4 below.



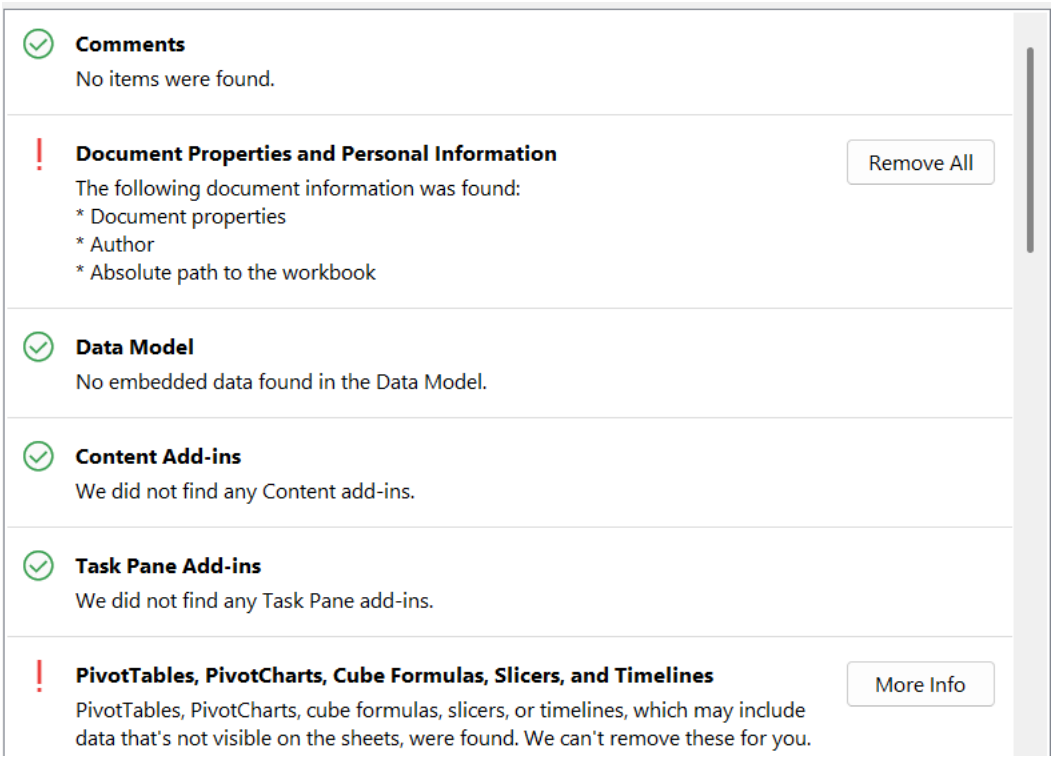
Unit	Grade	Grade Type	Grade Type Category	Reason	Start	End	Duration	Hours	Working Days	Contracted Hours	Department	Secondary Sickness Reason
zDemo1	Band 2 Healthcare Assistant	HCA	Unregistered	Asthma	19/07/2020 07:00	19/07/2020 23:59	1	11.5	1	23:00	-	Allergic (extrinsic) asthma

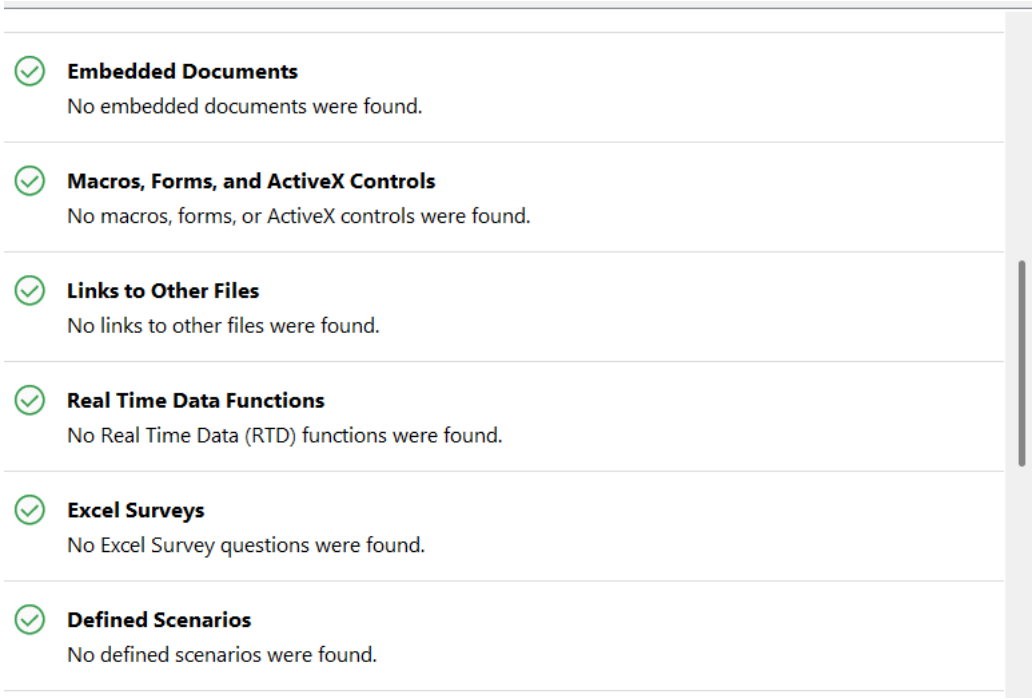
Figure 4 - Example row of information contained within the spreadsheet for the 2018 and 2019 fields

2.32. It is important to note that there was and is nothing immediately visible within the spreadsheet at first glance which shows that it contains hidden data or personal information. There is only one worksheet. Not all cells can be clicked into, to reveal underlying data (e.g. clicking on the cells in the adjacent columns shown in Figure 1 and

2.33. Figure *2* do not open the hidden spreadsheets). However, the file size of the spreadsheet is 2.75MB. This is larger than might be expected for the 'visible' data in the spreadsheet which totals approximately 2000 cells. Even then, however, it is not so large as to be patently obvious, and this assessment requires some knowledge of file sizes and what that is likely to mean in terms of the volumes of data within the file. In the version of Excel the investigators are using, it is only when one of the relevant cells is selected that the 'pivot table' work tools tab appears, and only when the cell is double-clicked into that the hidden personal data is visible.

2.34. In the course of the investigation, we have, in line with the ICO's guidance on using the 'Document Inspector' tool (see further, section 2.13 above), assessed whether the inbuilt tools in Excel will recognise that the spreadsheet contains the hidden data. The results of that are shown in Figure 5 below:


Comments
No items were found.
Document Properties and Personal Information
The following document information was found:
* Document properties
* Author
* Absolute path to the workbook
Remove All
Data Model
No embedded data found in the Data Model.
Content Add-ins
We did not find any Content add-ins.
Task Pane Add-ins
We did not find any Task Pane add-ins.
PivotTables, PivotCharts, Cube Formulas, Slicers, and Timelines
PivotTables, PivotCharts, cube formulas, slicers, or timelines, which may include data that's not visible on the sheets, were found. We can't remove these for you.
More Info


Embedded Documents
No embedded documents were found.
Macros, Forms, and ActiveX Controls
No macros, forms, or ActiveX controls were found.
Links to Other Files
No links to other files were found.
Real Time Data Functions
No Real Time Data (RTD) functions were found.
Excel Surveys
No Excel Survey questions were found.
Defined Scenarios
No defined scenarios were found.

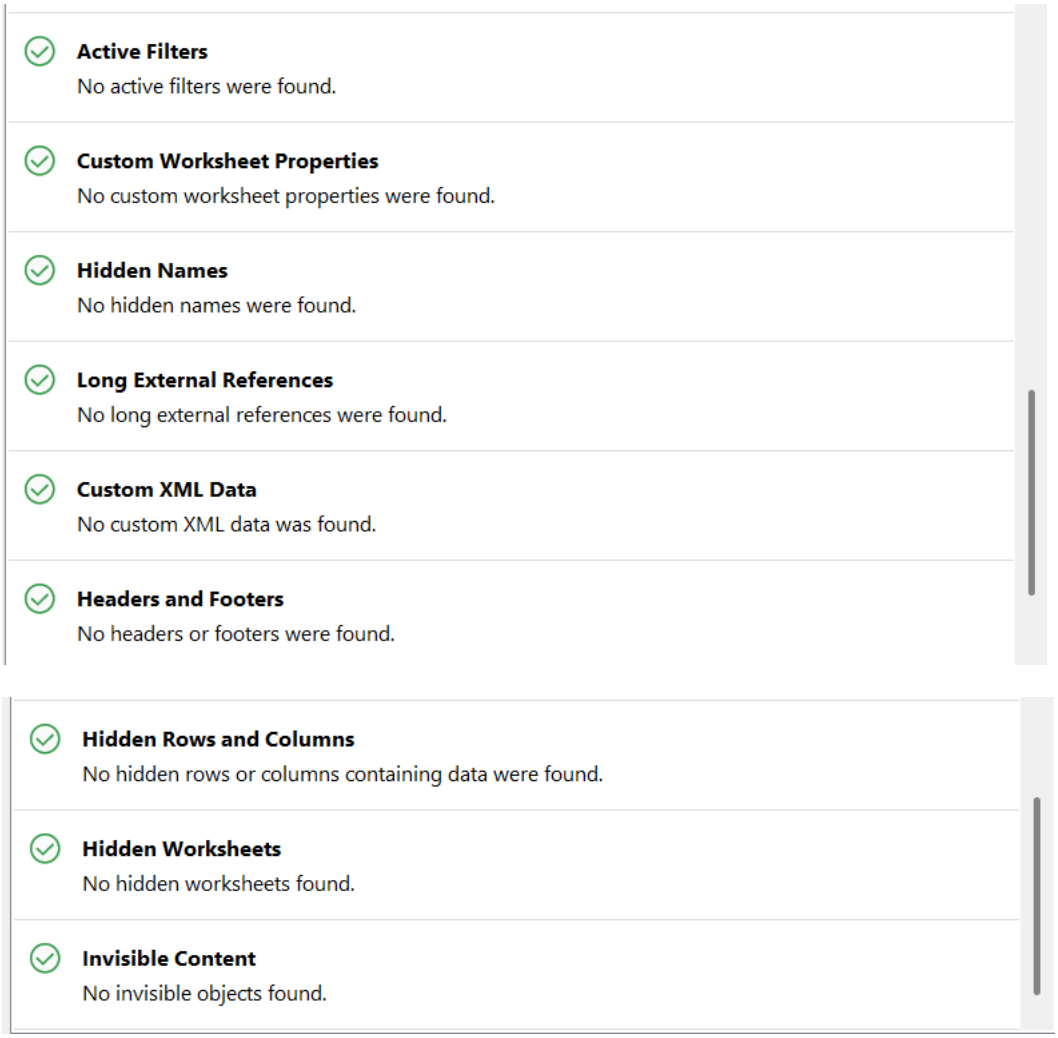


Figure 5 - Screenshots from the 'Document Inspector' tool applied to the spreadsheet disclosed in error

2.35. Many indicators commonly associated with hidden data, such as hidden rows, columns, worksheets or invisible content, were not flagged by the Document Inspector when applied to the spreadsheet disclosed in this case. Identifying the risk therefore required additional knowledge of the kinds of hidden data that can sit within spreadsheets.

2.36. Using the ‘remove document properties and personal information’ function does not remove the underlying data (i.e. the ‘personal information’ which could get removed are entries such as metadata of the author of the file, rather than the content of the spreadsheet itself).

2.37. The staff-member data is hidden in a pivot table, but this is not identified by Excel as a ‘hidden worksheet’ or ‘hidden row or column’.

2.38. As can be seen in the screenshots above, Excel does warn that there is a pivot table included (which is the issue at the heart of this incident). It does not, however, offer an automatic tool to remove the pivot table or warn that the pivot table contains personal data. The people involved in looking at the spreadsheet would need to know what a pivot table ‘is’, that they are considered ‘high risk’, and what to do in response to them (see further paragraph 0 below).

2.39. Accordingly, just using the ‘Document Inspector’ tool would not have prevented the incident from occurring in terms of removing the underlying data from the spreadsheet.

2.40. The investigators then re-saved the Excel spreadsheet (XLSX) file as a CSV (comma separated value) file. This reduced the file size to 6KB, and taking this step **did** remove any ability to access the pivot tables and the hidden data. This is the only way we have identified which would appear to actually remove the data which was exposed.

2.41. Finally, the investigators also used an enterprise-licenced version of Microsoft Copilot on the spreadsheet, to see whether it could identify that personal data was present. However, Copilot did not (in its initial pass) detect the pivot table and it was only when specifically prompted to look for it that it identified there was personal data in the spreadsheet. Accordingly, using Copilot would **not** provide a further safeguard in relation to this kind of data, and attempting to use general AI tools as a safeguard should be approached with extreme caution.

Who was affected?

2.42. The individuals whose information was contained in the spreadsheet were staff of RCHT, bank workers and agency staff, students from either placements at RCHT or seconded from Cornwall Partnership NHS Foundation Trust. Some of the staff on the spreadsheet were Kernow Health Community Interest Company (otherwise known informally as Cornwall CIC) employees, for whom RCHT was rostering their staff during this period.

2.43. During the incident response process, an analysis was undertaken by the Trust of the number of staff impacted by organisations. A fully anonymised version was provided to the investigation team and is as follows:

Staff Grouper	Unique People Impacted
RCHT Staff	7715
Students – External	122
CIC (111 service) – External	66
Agency – External	49
Unidentifiable[2]	51
TOTAL	8003

2.44. The hidden data was not directly relevant to the FOI response and was not intended to be disclosed in response to it. If an FOI request had been made for it, it would have been exempt from disclosure under FOIA.

[2] Unidentifiable' are staff members who, as a result of the discrepancies in the data and IT systems used, were unable to be identified in data stratification processes during the Trust's incident response. For example, they were listed under a specific team with initials, however, no person in the team at the time had those initials.

2.45. The data continued to be published on the Trust's website from February 2023 to November 2025. The Trust maintains 12-month logs of how many times webpages on its website have been accessed. Accordingly, it is not possible to say how many times the file was accessed between when it was published in February 2023 and November 2024 (being 12 months prior to when the incident was identified). In the period November 2024-November 2025 it was accessed 340 times. It was said during one of the staff briefings in response to the incident that this was 'slightly higher' than typical, but the investigators were unable to draw any conclusions from this. It is impossible to say whether the hidden data in the file was accessed by anyone accessing the file online, or if it has been copied or downloaded, and therefore any assessment of the risk here is hypothetical/conjectural. For instance, some access to the file may have been from automatic web-crawlers undertaking indexing activities, rather than any specific person.

2.46. On 17 November 2025, a member of the public who had accessed the Trust's disclosure log and the spreadsheet on the Trust's internet pages contacted a member of staff at the Trust via email, to say that they had found the hidden data. Paragraph 0 onwards of this report explains and considers what happened in response to the incident.

3. Investigation approach and terms of reference

The Investigation Team

Role	Initials	Job title	Dept/directorate and organisation
Investigation commissioner/convenor:	BG	Acting Chief Nursing Officer	Corporate
Learning Response Lead:	NB	Patient Safety Specialist	
Independent Investigation Team	TDS AL		Capsticks

Scope and Terms of Reference

3.1. The scope and Terms of Reference for this investigation are set out below. The conclusions in response to each of the terms of reference, insofar as they have been ascertained by the investigating team, are set out against these requirements, with explicit responses to points in the Terms of Reference highlighted as appropriate.

Scope

3.2. The investigation reviewed what led to the disclosure of staff information following a FOI request and also reviewed the incident response the Trust provided. The learning response also considered the impact upon staff but has remained separate from any personal complaints and claims processes.

Terms of reference

Part 1: Events leading and contributing to the incident.

- TOR1 Clarify the background of the individual/organisation requesting the information, the purpose, and justification for data use (e.g. patient safety review, compliance, audit).
- TOR2 Details on who may have accessed this information from data logs.
- TOR3 Understand the systems in place for sharing information with individuals, teams, or external bodies the data was shared, this should include the method of sharing (secure transfer, encrypted email, etc).
- TOR4 Any restrictions or conditions on use for this FOI request or other FOI requests.
- TOR5 Establish the facts surrounding the data breach incident including:
  - Identify how the breach occurred by understanding the system of work in place that resulted in the incident.
  - Who had access to the data (roles, not just names), How access was granted and monitored. Retention period and disposal process.
  - Assess the impact on affected individuals and the organisation.
- TOR6 Evaluate the adequacy of existing controls (including access. monitoring, retention and disposal processes) as risk reduction strategies.
- TOR7 Evaluate data incident response procedures to minimise impact.

Part 2: Learning and Improvement

- TOR8 Provide actionable recommendations for remediation and prevention by an independent SME.

- TOR9 Ensure compliance with relevant data protection regulations and reporting obligations.
- TOR10 To evaluate the Trust's response to the incident, including the learning from the effect on staff providing support to those affected/impacted by the data breach.

Summary of investigation process

3.3. The incident was brought to the attention of Information Governance via email who notified the senior executive team and the incident was reported on the Trust reporting system. A system-based investigation was commissioned with agreement from the Chief executive to follow the Patient Safety Incident Response Framework (PSIRF) due to the knowledge, skill and experience of the team in complex investigations.

3.4. An initial safety review was undertaken to ensure immediate improvements were in place, support scoping and commissioning of a further and more detailed investigation. This allowed terms of reference to be formed and the procurement of independent subject matter experts to lead the investigation with the support of the Trust's Patient Safety Specialist to act as Learning response Lead and ensure alignment with PSIRF.

3.5. The learning response team which included the independent subject matter technical experts identified key information sources, commenced memory capture and document review to inform the investigation.

3.6. Once complete, the PSII will go through the Information Governance Group and Patient Safety Incident Response and Oversight Group (PSIROG) for endorsement and approval, before sending to the investigation commissioner. The report will also be shared at JCNC for information. Actions will be overseen at the Information Governance group with oversight from the Quality Assurance

Committee. An approved copy of the report will be published for full transparency to those affected.

Information gathering

3.7. Information has been gathered from several sources to formulate the findings of this report. A systems-based methodology has been used to identify contributory factors which lead to the disclosure and evaluate the organisational response.

4. Findings: The Initial Incident

The FOI Request

Terms of reference 1 and 4

People Factors

4.1. The background to the individual requesting the information appears to be a journalist preparing a newspaper article about stress within NHS organisations. However, an individual does not need a particular reason for making an FOI request, and using FOI for data journalism is entirely legitimate. As we explore below, the issue in this case was the wrong information was disclosed by the Trust in response to the request (i.e. the information about individual staff was not what the applicant had asked for), as well as the actual response information.

4.2. There are effectively no restrictions or conditions of use on how information may be used in response to an FOI request normally. There is a hypothetical legal argument that a duty of confidentiality would attach to the parts of the hidden data disclosed in error and this should prevent the user from misusing it.

4.3. In practical terms, it is impossible to stop anyone from downloading and making their own copy of the FOI response spreadsheet or the information within it. Were this to have happened, this will not be known about by the Trust. As is set out elsewhere in this report, website logging tools available to the Trust say that the webpage was accessed 340 times in the 12 months prior to its removal, and the webpage was available for approximately 21 months before the logs begin.

4.4. In legal terms, there are no legal restrictions in FOIA itself over how the information may be used by those that are given access to it. There is arguably an implied ethical obligation of confidentiality that attaches to obviously confidential

information which has been obtained by a recipient in error. The obligation would arise if the recipient knew or had notice that the information is confidential, even if they did not actively seek it out or if it was disclosed by mistake. If they found it, a reasonable person would likely have regarded the information buried in the spreadsheet as having been disclosed in error, and having the necessary qualities of confidentiality about it, based on the substance of the information.

4.5. The investigators consider it likely that the email account used for the FOI requests was a temporary ‘burner’ account. Given the lack of response from when the Trust identified the incident and sought to contact the requestor via that account, the account was thought to be no longer in use or actively checked by the original applicant. The investigators triangulated the name of the requestor with other sources and identified an individual, believed to be a journalist, who they considered may be the original FOI applicant. The Trust established contact with that person via other contact details and requested deletion of the information that had been sent in error. Shortly after the investigation concluded, and just before the report was finalised, the journalist confirmed that the information had been deleted in accordance with the Trust's request.

Systems of Work

Terms of reference 2

Governance and handling of FOI requests at the Trust

Organisational factor: Information Governance Team structure

4.6. The Information Governance team at the Trust is structured as follows:

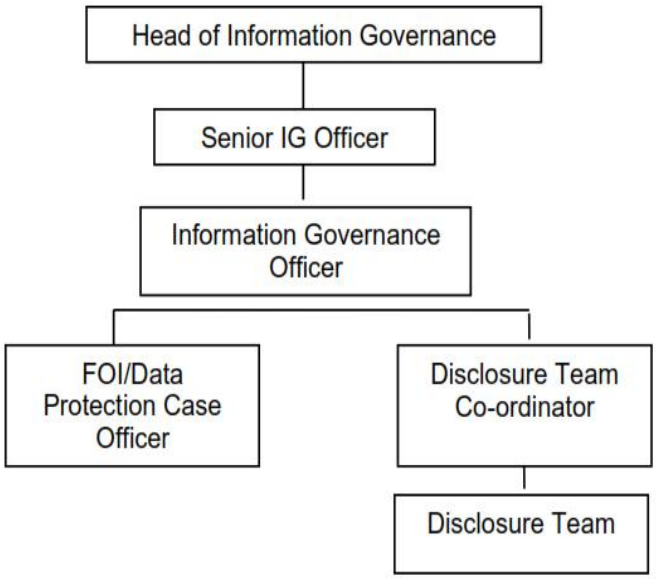


Figure 6 - Information Governance Team Org Chart

4.7. The FOI (Case) Officer[3] who was in post at the time of the incident no longer works at the Trust and therefore we have not been able to speak to them in the course of this investigation. The Information Governance Officer who was in post at the time of the initial incident has also left the Trust subsequently, and this role was vacant until 2026. Turnover of staff was raised as an issue by those we interviewed in this investigation.

[3] Although the org chart in Figure 6 uses the term "FOI Case Officer" most other documents, including the FOI SOP, use the term "FOI Officer" - which we have used in the report to describe the role.

4.8. We would observe that there is no standard approach to the role description of FOI officers nationally, in terms of the knowledge required for the role or the degree of autonomy associated with it. The Trust operates the 'FOI Officer' role at the more junior end of the spectrum, and this is reflective of the view of the role at the Trust as primarily an 'administrative' one. Other organisations place greater emphasis in the role including the application of exemptions and with a higher degree of operational independence, as well as in collating the responses and administering the process.

4.9. Day-to-day management of FOI requests sits (and sat) with the FOI Officer, while escalation and overall oversight rested with the Head of Information Governance. In practice, however, the Head of Information Governance was not generally involved in the routine handling of individual requests, but rather would be involved to assist in direct queries from the FOI Officer or those raised by information holders, during periods of absence if extra hands were needed, or if a request was made for internal review (so that there could be a 'fresh pair of eyes').

4.10. The FOI Officer has day-to-day responsibility for handling FOI requests. They co-ordinate the identification and preparation of requested information. The job description states that the FOI Officer "*will be involved in all aspects of administration of the FOIA process and processing of personal files and preparing them for disclosure to a tight deadline. The department is fast paced and would suit someone that can cope with pressure and has good IT literacy skills."* The evidence suggests that the FOI Officer's role was focused on checking that *"the relevant department answered all the questions"* and that they *"haven't missed something".*

4.11. During the investigation, we heard that more senior members of the Information Governance team were not routinely involved in deciding what information should be disclosed in each FOI response. Their role was primarily to provide advice and act as points of escalation where queries arose. In practice, questions would

ordinarily be raised by the FOI Officer first with the Information Governance Officer, then escalated to the Senior Information Governance Officer if unresolved, and thereafter to the Head of Information Governance where necessary. Responsibility for reviewing the accuracy and sensitivity of the substantive content of FOI responses sat with the department providing the information and in the relevant sign-off process with the executives.

Organisational factor: Information Use Framework Policy

4.12. Appendix 4 of the Information Use Framework Policy provides a summary of the FOI process in general terms. It does not touch on security of information or removing hidden information, however, in general terms it speaks to the process followed by the Trust in relation to FOIs:

(1) Summary of FOI requests.

(2) Identifying and recording a Freedom of Information Act request.

(3) Responding to a request.

(4) Applying exemptions and the public interest test.

(5) Refusal to disclose.

(6) Complaints / review processes.

Task Factor: FOI Standard Operating Procedures

4.13. In accordance with the SOP version 21 from March 2021, which was in place at the time of the incident, the usual process for responding to FOI requests was (in summary) as follows:

(1) FOI requests could arrive via multiple channels (email, letter, online form, PALS). Once sent to the FOI team, the FOI officer was expected to check

validity (name, contact address, FOI scope, clarity), note the 20-working-day deadline from the next working day, and if valid, log the request on the risk and incident management system (Datix) to generate a unique FOI reference number, and create a folder in the FOI Mailbox.

(2) The FOI officer would acknowledge the request within 48 hours (not including weekends) using a standard template and/or request further information if needed.

(3) The FOI officer would then collect the information by filling out the response template with the questions to be answered, identify the correct department and nominated FOI lead, and share the response template with them asking them to provide the relevant information (copying in the Care Group Manager). The FOI officer would provide clear deadlines, chase responses, and prepare the final disclosure.

(4) The FOI officer would then compile and finalise the response i.e. inserting departmental replies into the response section if they haven't been inserted already, updating header/footer, collating response etc. This step also includes preparing attached documents for sharing. In relation to Excel spreadsheets, section 7 of the SOP provides as follows:

"*Sometimes, information will be returned in 'Excel' format, if this format is essential to understanding the request (e.g. lots of data that may need to be sorted/extrapolated), or, has been specifically asked for by the applicant, leave in Excel form when responding; however, you must remember to 'prepare for sharing' to remove any hidden data (see instruction below).*"

4.14. In relation to Excel documents, section 7I of the v. 21 SOP provided that FOI officer should click in Excel: *file – info – check for issues (prepare for sharing) – inspect document) – proceed (with all options clicked) – in Document Inspector click 'remove all'* for any data located.

4.15. In this regard, the SOP in place at the time therefore corresponded with at least some of the steps set out in the ICO's guidance in force at the time, set out in paragraph 2.12 onwards above, and indeed the SOP specifically included a link to the ICO guidance in a section headed Handy Sources of Information/Guidelines/Advice. However, the SOP only described using the 'Document Inspector' tool (and specifically highlights the 'removal of personal information' feature within it). It does not discuss converting material to CSV to remove pivot tables or mention pivot tables expressly. The Trust has now put in place further alternative controls which do provide a higher degree of protection against this risk (see paragraph 5.2 onwards below). In the course of the investigation there was no evidence that there was any wider drift from the standard operating procedure. No other near misses or incidents have been identified and an audit of FOI responses as part of incident response did not identify any cases. However, it is also worth saying that this request was not perceived as being a particularly contentious one at the time it was received. The legal requirement of needing to respond promptly to FOI requests (together with the wider volume of work) is likely to have been a contributing factor in this case.

4.16. Prior to sending the response to the applicant, the SOP in use at the time (v. 21) stated that the FOI Officer:

"…should convert the 'Word' response template to Adobe PDF (when posting the response to the Disclosure Log, you will only use Adobe PDF documents, this includes conversion of 'Excel' worksheets/workbooks)."

4.17. Instructions are provided with pictures demonstrating how to do this. Instructions are then provided as to how to amalgamate the documents into one PDF. The SOP explains that the response will then be sent and published on the Disclosure Log of the Trust webpage Royal Cornwall Hospitals Trust / Internet / Documents Library / Freedom Of Information / Disclosure Logs .

4.18. This stage of the SOP was not followed at the time the FOI response in this case was given, and the information was published. The version of the spreadsheet published on the Trust's website was in .XLSX format, rather than PDF. In the course of preparing this report we have investigated processing the spreadsheet (limited to the main workbook) into a PDF. This has a file size of 435kb, and it appears that once this is done, it is **not** possible to click through to the hidden data. Had the conversion to PDF happened, the level of risk from disclosure of/publishing the spreadsheet would therefore have been much reduced. However, we would highlight that we are not able to give an assurance that the PDF does not still contain hidden data which it could be technically possible to access, albeit it is plainly much harder to do so than where the data in the native (.XLSX) format. To our knowledge, CSV format, which is one of the simplest ways of formatting information (albeit which is still openable and workable in Excel) is the only way of positively confirming that there is no hidden data, and this is a step which is repeatedly highlighted in the ICO's guidance above.

Tools and Technology Factor: Use of digital technology

Terms of reference 3, 6 and 8

4.19. The Trust should note (and disseminate) the limitations of using and relying on the 'Document Inspector' tool as a control measure against accidental disclosures. Relevant staff should be trained further in how to identify pivot tables, the risk they pose, and how to remove them. This is relevant for staff involved in the FOI response process, but we also recommend that the Trust should undertake a wider training needs analysis of other staff that might be routinely collating, working with, publishing or sending out information in large datasets/data files (e.g. business intelligence roles, communications and other governance roles) to potentially untrusted or large groups of recipients, so that they are confident in understanding what data may be being disclosed. We note the Trust has produced some internal guidance on this issue, but it would be beneficial to consider how this is disseminated and for active training to be given on its

application to relevant staff. We understand that a different pivot table incident involving the accidental disclosure of personal data to a contractor working with the Trust had previously been raised in the summer of 2022 (albeit not in the context of FOI) and this indicates that although the potential impact of disclosure of such data under FOIA is typically regarded as more significant (as it is 'disclosure to the world', as set out in paragraph 2.6 above), the underlying problem of the wrong data being included and disclosed in data files is more universal. Again, we emphasise that wider use of Sharepoints and other systems which allow access to data to be restricted or removed (rather than emailing data backwards and forwards) can provide a degree of technical protection after an incident, but addressing the underlying problem is multifactorial and requires staff to understand and identify pivot table risks. More training (on a needs-assessed basis relevant to job roles) and wider resources on this issue may assist. However, there is a paradox that the staff that work most often with pivot tables will be more attuned to the risk than staff that work with them uncommonly, but who are less likely to have training.

4.20. The spreadsheet was shared in 'open' (non-encrypted) email with the recipient and then posted on a public website. This is common for FOI responses and promotes interoperability of the information. Simply sending the email in an encrypted or password-restricted format would have had a minimal impact on the incident here, because (1) it was the posting of the material on the website which posed the wider risk of access, and (2) even if the email had been encrypted, the wrong material would still have been in it. It would be open to the Trust to consider using an encrypted email format or file transfer system for FOI responses, which could provide an additional safeguard in enabling the Trust to remove access to any file in terms of it being (re-)downloaded, if an error is found within it. This would not, however, prevent inappropriate material from being included in the first place.

4.21. **Recommendation**: It is recommended that wherever possible, data files should be disclosed in a CSV format (and if the Trust considers it appropriate, the CSV file converted to PDF). This is most reflective of ICO guidance, and CSV files also potentially assist with promoting the interoperability of data (i.e. it can be harder to accurately copy data from a PDF). Prior to sending data files externally (or published on the Trust's website) the underlying file should be saved as a CSV, opened, and the 'Document Inspector tool' re-run on it, to check for any information which should not be included within it. This should be verified by another member of staff. This step can be taken in conjunction with the other controls that the Trust now has in place (see section 5 below). The FOI SOP and other relevant policies should be updated accordingly.

4.22. These safeguard steps are ultimately human-reliant organisational measures and 'soft controls'. The Trust should consider whether there are further 'data loss prevention' tools (technical IT measures, including any automated steps – although note paragraph 2.41 above) which could be used to seek to stop inadvertent or inappropriate disclosures of information (whether in the FOI context or more generally). However, the investigators appreciate that the Trust is an organisation which needs to communicate rapidly and effectively with patients, the public, clinicians elsewhere and partner organisations, and this will include the need for sharing of information including identifiable information in spreadsheets and other formats. Any deployment of additional technical or organisational measures designed to minimise the risk of inappropriate data being disclosed elsewhere must not make the **appropriate** exchange of information more inefficient or ineffective. A careful risk-benefit analysis and operational impact analysis would need to be undertaken before any such measures are deployed.

4.23. **Recommendation**: The Trust's web design team should continue to assess the extent to which any webpages on the Trust's website should not be indexed or automatically findable and consider controls to minimise the vulnerability of such systems, in line with NHS cyber security guidance, good practice in external attack surface management and wider penetration testing.

Task factor: Freedom of Information Guidance for Information Holders

4.24. The FOI Guidance for Information Holders is provided to the 'spoke' staff, who are responsible for gathering information, along with the wording of the FOI request itself. The document explains the responsibilities of Information Holders and sets out the key legal duties to identify whether information is held and to provide it within the required timescales. It also gives practical guidance on how to interpret requests, carry out thorough searches, seek clarification where requests are unclear, and handle situations where answering would exceed the cost limit.

4.25. In addition, the document outlines how to assess concerns about disclosure, including applying exemptions (primarily referring to instances where information is commercially sensitive and the public interest test where relevant). It also answers common questions about extensions, inaccurate information, response formats, and complaints or reviews.

4.26. However, this guidance does not mention provision, protection or removal of personal data.

4.27. The Guidance also says, "*You should send rch-tr.foi@nhs.net the information in the Word response template unless otherwise specified in our request to you."* It is unclear whether this means it is expected that the information handler should copy any and all information for an FOI response into Word (and at least one staff member appeared to think so during interviews undertaken during the investigation). Depending on how the information is formatted, conversion to Word might provide a partial guard against inadvertent disclosure. However, embedding material from other formats into Word files can also present a risk, because it can also preserve the original underlying data, and because the data is then embedded in a Word document an additional layer of complexity or ineffective 'masking' of the data is applied to it. We therefore do not regard it as a particular problem that FOI information is not returned to the FOI team solely in a Word

format, as long as steps are then taken to protect the data before it is disclosed. Irrespective of the risks and benefits of copying material into Word, it would appear both from the way this request was handled, and the terms of the FOI Officer SOP, that the general expectation was that that information could be returned to the FOI team in an Excel format (rather than simply Word).

4.28. The Guidance for Information Handlers does not itself discuss steps to take to protect Excel spreadsheets or other formats of data provision. There therefore is a tension between the expectation described in paragraph 4.43 and shared by some staff members, which was that the department providing the information should be checking that the information is appropriate for disclosure, and the lack of documentation to this effect in the FOI Guidance for Information Holders. It may be prudent for the Trust to also consider explicitly requiring the 'upstreaming' of the conversion of datasets into a CSV format, as an additional control, by updating the FOI Guidance for Information Holders. In this way, the entire FOI/IG team, in collating the response for publication, will be looking at the version of the material for potential publication 'with fresh eyes' as a way of managing the possibility of inadvertent disclosure.

System Weaknesses: Key Contributory Factors (CFs)

Organisational, Task and People factors -

Term of reference 5 and 6

CF1: Allocation of 'Information Holder' staff responsible

4.29. Appendix 2 of the FOI SOP includes a contacts list for FOI requests. The investigators heard that the FOI contacts list is, in practice, an aid for the FOI officer. It is not meant as a prescriptive list of those who should be contacted. There will be names of staff who the team know can provide cover or assistance beyond that list. This includes requests relating to HR related issues. In

accordance with this SOP, the FOI request was circulated by the FOI officer to the relevant member of the e-rostering team. The FOI officer also copied in the People Information Unit (PIU) central mailbox and a further colleague (Member of Staff 2). We note that neither the further colleague who was copied, nor the PIU mailbox, are on the main distribution list in the SOP, and therefore were likely included by the FOI Officer based on previous/informal practice. The FOI Officer requested a response by 6 February 2023

4.30. It appears there was initially some uncertainty about ownership of the response to the request, and which team was responsible for providing the relevant information. Clarity was sought through email exchanges between staff on who was best placed to respond to the FOI request given the information required and capacity to respond within the 20-day window. As a result of that exchange, the FOI request was redirected in full to the Rostering team with a return date of 6 February.

4.31. During the investigation, the significance of this transfer and the implications for how the FOI was handled was highlighted as the PIU were identified as holding greater expertise in complex data management and associated tools, therefore relying on rostering, who were less experienced in this inadvertently introduced additional risks in data handling.

4.32. The expertise of PIU in handling large datasets and responding to potential breaches is highlighted by evidence of a previous incident in which PIU service manager identified hidden data within a pivot table shared by People Partners. This was flagged immediately with the relevant People Partner and Head of Information Governance for resolution, and further guidance was also given to both parties around the use of pivot tables. In January 2022, concerns were raised internally about a pivot table that had been shared externally, which contained embedded personal data that could be revealed by interacting with the spreadsheet. It was specifically noted that the functionality of pivot tables was not

fully understood by those authorising the disclosure, raising questions about whether informed approval had been given. This earlier incident demonstrated a known risk associated with handling complex spreadsheet outputs without adequate technical understanding, although the investigators have not identified any particular evidence to suggest it was actively being considered in relation to the FOI request in question.

4.33. Against this background, the process of responding to the FOI request in question involved extensive data extraction and manipulation within large Excel spreadsheets, work that would ordinarily fall within PIU's remit. The investigation heard mixed evidence regarding whether such complex Excel outputs would typically be within the remit of PIU or rostering. Ultimately, it seems that Rostering held the information but not the experience, and PIU had the experience but not all of the information. The fact that the request was ultimately handled by Rostering, a team without equivalent training or system ownership, demonstrates a potential misalignment between the technical demands of responding to the FOI request and the expertise of the responding team. In circumstances where similar data-handling risks had already been identified historically (we understand this learning was not shared with the rostering team), this allocation to them likely increased the risk of errors and inappropriate disclosure. Ideally both teams would be equally experienced in handling large datasets such that they would both be comfortable handling a request, or the rostering team compile the information for PIU to process.

4.34. **Recommendation:** The Trust should review its FOI handling request process to ensure an agreed route for requests which aligns asset ownership with data handling expertise. Training on handling large excel spreadsheets should be provided to teams that are responsible for collating information in large quantities, or an agreement for support with data expertise. If informal relationships have developed or are being used to collate material in response to FOI requests, they should be standardised into the policy documents to ensure appropriate training is completed for the staff involved.

CF 2: Creation of the spreadsheet

4.35. The rostering team prepared the information. Due to the passage of time, it is difficult to ascertain how exactly the information was collated. The investigators heard evidence that two different staff from the Rostering team prepared the information. The investigators heard there was some confusion as to where the data had been downloaded from, the eRostering system and electronic staff record were possible sources however, concluded based on feedback that the data was most likely extracted from the eRostering system. For clarity, eRostering is not the same IT system as the Electronic Staff Record (ESR). Although they are two distinct IT systems they are interconnected; whilst e-rostering generates day to day schedules and attendance (including reasons for absence), the data is then integrated into the central ESR to ensure matters such as pay and workforce reporting are performed. The data extraction from eRostering is identifiable from the pivot table (rows) data released, as well as the column titles in the underlying data – the row acronyms for grade and job role only exist in the eRostering system as do some of the other column headers. Another identifier that the data was roster data is that CIC, students and agency were included. The investigation heard that this information would ordinarily not have been found on ESR.

4.36. The data was analysed to prepare information relevant to the FOI request. The information relevant to the FOI request was synthesised into the final pivot table. The investigators heard that this is the process followed by e-rostering when sending information to remove the raw data and only supply information without any identifiers. We heard that pivot table was then likely copied into a new Excel spreadsheet. At the time of the incident, the team believed that this process would prevent sensitive information from leaving the department, they do not send raw staff data to the FOI team, and therefore the team attempted to remove the raw information and only send the high-level pivot chart. It is unclear why some information from 2019 and 2020 had been anonymised prior to analysis; it was hypothesised that both members of the rostering team contributed to the analysis, one doing the first two years and the other doing the last three, and then one of

them doing the final copy paste to the new spreadsheet and providing it. If this was an attempt to cleanse the data, it would have been helpful for a warning to have been given to the FOI team that this had been done. Though the investigators heard that given the team considered the raw data had been removed (and were unaware of the dangers of pivot tables) they did not consider this would be required as there was no concern about sensitive data potentially sitting within the spreadsheet. During investigation interviews, one member of staff highlighted that the FOI material should have been put into a Word document, demonstrating that there was no certainty about the proper format in which information should have been provided back to the FOI team.

4.37. There was no intention to send personal information to the FOI team. Exclusion of the individual sickness information before the data was returned to the FOI team would represent a 'first safeguard' in an FOI response, i.e. the information provided back to FOI team to collate the response to the request would then be in essence 'fit for purpose'. However, because the e-rostering team were unaware of the risks of hidden data lying behind pivot table, they considered that this 'first safeguard' had in fact been successful. Further training should have been provided to staff handling large datasets on the risk of hidden data being found behind pivot tables, to ensure the safeguards in place did not fall through as they did in this case.

CF3: Processing of the FOI request by the Information Governance team

4.38. On 30 January 2023 at 15:12 the information (including the Excel spreadsheet) was returned by a member of the e-rostering staff to the FOI Officer in the information governance team. At 15:46 the same day (around half an hour later) the FOI officer sent the information on for checking.

4.39. Evidence provided confirmed that, at the time, there was a clear Standard Operating Procedure governing the release of Excel spreadsheets. As mentioned above, section 7 of the SOP provides as follows: *"Sometimes, information will be returned in 'Excel' format, if this format is essential to understanding the request (e.g. lots of data that may need to be sorted/extrapolated), or, has been specifically asked for by the applicant, leave in Excel form when responding; however, you must remember to 'prepare for sharing' to remove any hidden data (see instruction below)."* Section 7I of v. 21 of the SOP provides that FOI officer should click in Excel: file – info – check for issues (prepare for sharing) – inspect document) – proceed (with all options clicked) – in Document Inspector click 'remove all' for any data located. As is set out above, however, the Document Inspector does not include an automatic response to a pivot table. The SOP went on to say that all material should have been converted to PDF before the response was sent out.

4.40. It is reasonable to conclude that the required steps were not completed as expected by the FOI officer role, given the occurrence of the data breach and that the document was not converted to PDF. If those checks had occurred comprehensively, there would have been a potential opportunity to identify the hidden data and remove it from the final Excel spreadsheet disclosed. As set out in paragraph 4.19 above however, the comprehensive **removal** of information (rather than simply reformatting it in a way which makes it hard to access) requires some knowledge of the necessary action to take in response to pivot tables which Excel does not do automatically.

4.41. We considered that v. 21 of the FOI SOP (or its practical application) had some ambiguity as to whether these checks should be done before or after the response was sent to colleagues for sign-off – see further paragraph 4.43. In our view, it is preferable for this to occur before sign-off, because then the information is presented for sign-off in the format it will be disclosed to the applicant, and it avoids a single point of failure at the very end of the FOI process. The current version of the FOI SOP (v. 26) explicitly says that checks should be undertaken

before sign-off and therefore addresses this risk. We note that this is confined to Excel spreadsheets and the Trust should consider incorporating a similar process for other redacted (exempt) material.

CF4: Approval / Sign off

4.42. On 30 January 2023 at 15:46, the information requested, including the accompanying Excel spreadsheet, was sent to the relevant Senior Manager for an accuracy check. On 31 January 2023 at 16:25, the Senior Manager confirmed that the information was approved, subject to executive approval. Following this accuracy check, the information was forwarded on 1 February 2023 at 08:17 to the relevant Executive Officer, for executive-level approval. The Executive Officer confirmed their approval at 09:02 the same morning. Subsequently, at 12:30 on 1 February 2023, the information (including the spreadsheet) was returned to the applicant.

4.43. The investigation heard that the head of IG would have expected the ‘check for appropriateness of sharing’ process should have been completed by the FOI officer before the information was escalated for approval/sign-off. Therefore, the head of IG would not have expected executives to be checking for hidden data as part of their review. This was affirmed by the Executive Officer who undertook the sign-off, who described the executive review process as focusing on whether the information aligned with the requester’s questions, whether a complete response had been provided, and whether there were any potential concerns relating to communication, reputational impact, or adverse media. The Executive Officer also noted that data protection considerations were addressed through the Trust’s standard data protection policies and that Executive Officer assumed any pivot tables or hidden data had already been removed prior to executive approval.

4.44. The sign-off process was a potential opportunity for there to be a ‘third’ layer of check which could have identified the hidden data. However, formal checking of

the material for extraneous information was not incorporated in the FOI processes at the time of the incident, and so it is not surprising the hidden information was not identified. In terms of current practice and in light of the incident, it seems that executives (also) checking for hidden data has now become a standard but undocumented/informal practice. For instance, the investigation was told that one executive saw '*an example from another colleague the other day where somebody was trying to provide a spreadsheet and I saw that executive colleague pushing back.'* Equally, however, the final sign-off process is often done under time pressure and therefore there is a competing imperative to finish responses. Those that are undertaking sign-offs do not have dedicated/protected time in which to do it.

4.45. **Finding:** There was a large chain of people involved in collating the FOI response. There is no evidence of inappropriate access to data; those that had access to it had routine access as part of their roles. However, no-one appears to have considered (or at least actively communicated) that the spreadsheet might have been tainted with a pivot table. It is likely that the people further down the chain were not aware that the pivot table was included, and/or in any event, had assumed that the spreadsheet had been checked further up the chain. The ultimate responsibility for checking this in the SOP, however, was with the FOI Officer.

Training and supervision of FOI officers

4.46. The FOI Officer role description appears to be intended to be primarily administrative. Training was described as comprising the following main elements:

(1) FOI training QTC/BCS

(2) a comprehensive SOP setting out the FOI process in detail (i.e. the SOP described in paragraphs 0 to 4.18 above); and

(3) iterative, tailored on-the-job training adapted to the individual's experience and needs.

However, the junior/'administrative' nature of the role means that in practice, the FOI Officer role was not designed to be working as an autonomous subject matter expert in FOI. There is a tension or ambiguity in the role, in that the expectations were that the FOI officer was able to apply FOIA, and also, they would make decisions on disclosure (rather than more senior colleagues) with limited operational supervision. More generally, there had been a high turnover of staff within the information governance team and the team more generally is responsible for a number of information rights response processes with statutory time limits with overwhelming levels of demand.

4.47. In relation to point (3) above, the investigation heard that training was 'on the job' delivered in a practical, informal and step-by-step way. The FOI Officer in place at the time would sit with the Information Governance Officer colleague, who would demonstrate each stage of the process and run through the role with them. This would progress to the FOI Officer dealing with some FOI requests themselves and the Information Governance Officer supervising them as they completed tasks themselves, such as logging a new FOI request. This allowed the 'trainee' to learn the process gradually while receiving immediate support and feedback.

4.48. If at any time clarity was needed or a pattern of not adhering to process was raised, it was expected that additional supervision would be given informally or formally through a personal development plan to support consistent and compliant practice.

4.49. We spoke to a more recent FOI officer who had a similar experience of training and supervision to that described above as being in place at the time. However, throughout their own tenure, the IG Officer role was empty, so the more recent FOI Officer reported directly to the senior IG officer and Head of IG. The more recent FOI officer role also saw the FOI officer role primarily as administrative and,

after about two weeks of hands-on training with the previous FOI officer, felt able to understand the general patterns of the processes. While the more recent FOI officer did not have a dedicated work buddy, they did receive support and guidance from colleagues whenever they were unsure or found tasks complex. They pointed out that *'everything starts and ends with the SOP'* and so they followed this closely. They confirmed that in accordance with the SOP they would check for macros, remove them, save the file, and then send it for approval.

5. Changes to information governance arrangements for publishing FOI responses since the breach

Terms of reference 6

5.1. An updated version of the FOI Officer SOP (v. 24) was published in September 2023. The current version of the FOI SOP (v. 26) was published in February 2026.

5.2. In relation to Excel documents, section 7I of the SOP now provides that after completing the 'prepare for sharing' checks, the FOI Officer must lock/protect the Excel workbook, with an illustrated description of the process to be followed to achieve this:

a) You must always lock/protect the Excel workbook before disclosing.

b) To lock the Excel workbook: Review - Protect workbook - Add password.

c) Then 'save' the workbook.

d) This has now protected the workbook, and any hidden data is now inaccessible.

e) Any request where there is an Excel document forming all or part of the response must be sent to [senior staff members in the IG team] to obtain sign off ahead of the Executive approval for disclosure.

f) Once the Excel has been approved by [the senior staff members in the IG team] then the request can be sent for Executive approval as per the SOP.

5.3. We have tested this approach using the spreadsheet which is the subject of the incident. Password protection does prevent the hidden data in the spreadsheet from being accessible to others, and therefore provides an effective combination of controls (in conjunction with the 'second pair of eyes' safeguards used by the Trust to ensure that it has been applied correctly). It therefore seems that the Trust has put in place a reasonable control and this conforms to multiple elements of the ICO's current guidance described in paragraph 2.17 above. However, we note that when taking this approach, the Excel file size still appears to be 2.75MB

which means that the personal data is presumably still 'hidden' within it (but simply has been rendered technically inaccessible without the password).

5.4. On 27 November 2025 (and in light of this incident), the Trust Information Governance Team circulated via email a revised protocol for managing FOI requests, including involving spreadsheets. This also included the conversion of Excel spreadsheets to CSV as an additional control. In this regard, therefore, the arrangements that the Trust has put in place subsequent to the incident comply generally with the principles set out in the ICO's current guidance on minimising inadvertent disclosure of information in spreadsheets (i.e. multiple controls, including the use of passwords and file conversion), although the FOI SOP itself (v. 26) does not include the 'convert to CSV' point. It would be prudent to clarify whether this is still required, and to update the FOI SOP if so. We recommend that it is.

5.5. The Trust could also expressly integrate the ICO checklist described in paragraph 2.19 above into its processes as well.

5.6. Going forward, we recommend that the Trust substantively updates its other policies and procedures to incorporate the steps set out in the email described at paragraph 5.4 to ensure there is permanent adherence to these arrangements. The disclosure log on the Trust's website does appear to still include some older .XLSX files (the disclosure log webpage appears not to have been updated online since August 2025, and older files have been removed, but there are various spreadsheet files online for the period 2023-2025)[4]. However, in light of the incident, we understand an audit has been undertaken of spreadsheet material on the Trust's website to assess whether any personal data has been inadvertently disclosed, with no high-risk material located (see paragraph 6.9(15) below).

[4] Publishing an FOI disclosure log is not a legal requirement.

5.7. The context in which this incident occurred was an FOI response, but the nature of the organisation means that there may be disclosures of other large data files within the Trust. The PIU lead has produced a helpful guidance note entitled *"Data sharing tips, tricks and pitfalls* ", which is not specific to FOI issues. We recommend that this guidance is disseminated more widely within the Trust. The E-rostering team have also implemented an SOP setting out clear guidance on how information should be prepared, what data must be removed, and the correct processes for securely sharing information going forward. Consideration should be given to assessing which members of staff are more routinely involved in data sharing exercises and this guidance (and the opportunity for additional training) targeted towards them.

6. Findings: Responding to the incident and Incident management

Terms of reference 5, 7 and 10

The personal impact of the data breach

6.1. It is first appropriate to mark the sensitivity of the incident for many of the individuals affected, and the impact in terms of compounded harm (for instance, where a staff member had a sensitive or enduring health condition or personal circumstance to begin with), only for this to be 'broadcast to the world' in the spreadsheet disclosed. Whilst it is important to note that no financial, bank account, national insurance number, address, date of births or contact information were included in the spreadsheet, and the Trust sought to communicate this], many staff were left very upset by the actual information that was disclosed and have said that it undermined their trust in the organisation. Some staff appear to remain uncertain about what was actually disclosed (i.e. they remained concerned that financial or other personal information had been disclosed). This illustrates the challenges in trying to communicate effectively the details of a data breach at scale. Furthermore, managing the incident itself had a serious emotional impact on staff who have worked on it – particularly those working in the call centre, who found the experience very difficult and without feeling they had much agency in their involvement. Sadly, some members of staff who were upset by the incident itself did not always behave kindly to colleagues involved in the response.

6.2. The work and effort undertaken to respond to the incident and personal sacrifices undertaken by many staff to seek to address the incident were commendable. Senior staff told the investigators how proud they were of the staff who contributed to the incident response. Although we note (see paragraph 6.48 onwards below) that some staff surveyed in response to the incident felt that the Trust was not transparent enough about the incident, we consider that the Trust met and sought to exceed its legal duties in relation to the management of the incident, and to be as candid as possible about what happened. Nevertheless, some staff questioned

the sincerity with which the Trust said sorry, or considered that the actions did not match the words.

6.3. Overall, we consider the Trust mobilised efficiently and effectively in a difficult situation. The Trust was able to notify an extremely large number of people about the incident, and used a range of methods to seek to do so. The Trust's existing incident management processes provided a framework which worked overall but this was an incident without precedent. There is no single or perfect way of responding to incidents such as this; decisions which overall were taken with a view to ensuring a comprehensive and timely response left some people unhappy. Any shortcomings addressed below are for the purposes of ensuring constructive learning going forwards.

6.4. The Trust maintains a Data Breach Policy and the overall response to this incident accords with the framework provided by that policy, although it would appear that this policy is designed for smaller incidents. A mass cyber or data loss event should be factored into the Trust's business continuity exercises and a closer link drawn between the Trust's Data Breach Policy and business continuity or Emergency Preparedness, Resilience and Response (EPRR) arrangements. The scale of this incident meant that there were departures from the Data Breach Policy, ordinarily to take a more involved approach to incident management.

6.5. We have considered the Trust's Emergency Preparedness, Resilience and Response (EPRR) Strategy. We understand that consideration was given to whether the incident should have been considered a 'critical incident' under that framework, and some contributors to the investigation were disapproving of the decision that it was not. The definition of a critical incident within it is *"any localised incident where the level of disruption results in the organisation temporarily or permanently losing its ability to deliver critical services, patients may have been harmed or the environment is not safe requiring special measures and support from other agencies, to restore normal operating functions."* By reference to this

definition, we do not consider that the threshold for declaring a critical incident was met here (in other words, the Trust legitimately concluded that this was not a 'critical incident'), although this conclusion should not detract from its seriousness. We have been informed that aspects of the critical/major incident response process were incorporated into the Trust's response. We have also considered the applicability of the Civil Contingencies Act 2004 (CCA), which requires NHS organisations and providers of NHS-funded services to show that they can deal with large-scale emergency incidents while maintaining services. However, we do not consider that this type of event would have reached the threshold for it to be considered an "emergency" to which the CCA would apply.

6.6. That said, the numbers of staff affected and the resources needed to manage the incident were very significant and at times were significantly underestimated by the Trust, and some of the limitations of practical resources (e.g. space within the hospital) meant that staff 'on the ground' found the incident difficult to deal with. Some said they felt under-supported, and that the failure to call a critical or major incident meant that the pressures of other work remained present and dedicated resources (e.g. an appropriately sized incident management centre) were not available. Some staff members gave up holiday or worked long after hours or over weekends in order to contribute to the response. As one staff member commented, *"it's typical NHS, it runs on goodwill".* The Trust should factor the experience from this incident into its business continuity response plans, particularly in cases where only one staff member has specialist knowledge of systems necessary for incident responses. This leads to overreliance on that individual and poses a failure-risk in future cases (for instance, if that individual is unavailable for whatever reason). Ensuring there is training and knowledge sharing amongst staff, and effective deputization arrangements, is very important.

6.7. Necessarily a response to an incident of this kind will be evolving/iterative. Choices had to be made about the allocation of staff time and in the case of some staff that would normally work with patients, their working day was reallocated to working on the incident response. Some of those staff felt that they consequently

had let patients and their families down, because meetings had to be rearranged or work reprioritised so that they could contribute to the incident response process.

Context: morale among some staff affected by the incident

6.8. The investigators have been told that the incident came to light during a period of organisational change, triggered in part by the Trust's need to deliver a cost improvement plan of £49.3m, and which had included a proposed redundancy/restructuring programme affecting some staff. This context then impacted negatively on some staff morale and behaviours in the course of managing the incident.

Timeline of incident response

6.9. The following is a general timeline of key steps which took place in the incident response. A very wide range of incident response measures were operating in parallel/quick succession, particularly during the early phase of the incident response. A more comprehensive list of the various strands of response are helpfully set out in greater detail in the Trust's documented action plan/task-and-finish tracker, which we do not repeat in full here. Having described the key steps undertaken, we discuss various elements of the response in greater detail, so as to seek to provide 'lessons learned' for the Trust:

(1) 17 November 2025, 11:23: The existence of the spreadsheet was reported to the Trust via email, by a third-party member of the public who had accessed the Trust's disclosure log on the Trust's internet pages on 17 November 2025. However, the individual that was contacted had been on annual leave and so the email alert was not picked up until 19 November 2025.

(2) 19 November 2025: On discovery of the reported incident, various actions commenced immediately within the Trust to handle it and liaise with affected individuals. An incident report was submitted on the same day of discovery. The Trust's Head of Information Governance was to prepare an executive briefing paper, so they could be made aware of the incident.

(3) 20 November 2025: The incident was added to Datix, under reference R254194. A review was commenced of all previously disclosed Excel sheets to establish if further incidents had occurred. The investigators understand that the Trust sought to contact the original FOI applicant, to ask that they delete the original response (see further, paragraph **Error! Reference source not found.** above).

(4) 21 November 2025, 14:56: A Data Security and Protection Toolkit Incident Report was made, which is standard for NHS information governance incidents, and automatically makes a referral to the ICO where inbuilt relevant thresholds are met. The incident report noted that changes were being made to the FOI SOP to ensure no future Excel sheets are disclosed without being converted to PDF-type documents. The Trust established a project working group/incident response cell, led by the then Chief Executive, to oversee the response to the incident. The Trust's internal communications team was notified. Contact was also made with the Trust's external legal advisors, for advice on incident reporting and management.

(5) 22 – 23 November 2025 (weekend): The Trust briefed its specialist external communications advisors, to start the process of preparing the communication strategy for notifications to affected staff and incident management.

(6) 25 November 2025: The Trust received confirmation from the ICO, deciding no further action will be taken and the case was closed from their perspective. An executive meeting brief was prepared with a further executive briefing meeting taking place on 27 November 2025.

(7) The Trust developed its initial communication strategy based on a stratification of the staff members concerned and risk associated with the data.

(8) 28 November 2025: The People Information Unit was asked to start doing historic data sweeps of staff lists and ESR to capture everything (and this work in turn was picked up by People Information Unit (PIU) Service Manager on 1 December 2025). A computer coding script was developed and applied to categorise the severity of sickness information by reason. This was done so that the Trust could seek to identify those with high/very high severity risk sickness information overall, as well as severity for each reason published per person. This was considered important for the appropriate first degree of interaction and support for staff members concerned. The communication strategy was that all staff working for the Trust affected by the incident would be emailed, all-staff briefings would take place via Teams meetings which staff could attend, and a call centre would be set up primarily to deal with the most sensitive cases where direct contact was considered appropriate.

(9) About 1 December 2025: a script was prepared for staff who had been allocated to work in the Trust's incident response call centre to assist with notifications to staff. A rota was drawn up for staff to work in the call centre. Call handlers were briefed on 2 December 2025.

(10) On and around 1 to 3 December 2025: various briefings took place with key organisational stakeholders, including the JCNC staff-side negotiating committee.

(11) 3 December 2025: The Trust call centre went live.

(12) The Trust wrote (initially via email, but also through hard-copy correspondence) to approximately 5000 current staff and 3000 former staff to apologise for the error and explain what had happened.

(13) The Trust provided phone support initially envisaged to be for those identified as having high-sensitivity data within the spreadsheet.

(14) 5 December 2025: The Trust carried out MS Teams Live question and answer sessions with staff which commenced on 5 December 2025 with daytime sessions and one evening session to communicate what had happened. The Trust also created a frequently asked questions page on the Trust's intranet which included a recording of one of the Teams videos, and an update page

was also set up on its external website, which went live on 15 December 2025. The Trust sought to describe the incident and assure staff that no financial, bank account, national insurance number, address or contact information was breached.

(15) Cornwall IT Service (CITS) carried out an independent review of the FOI portal and found no other breaches of personal data. The Trust also identified an archived copy of the FOI response on a government-hosted web archive, which was taken down on the day it was identified. During interviews, we were advised that no copies of the FOI response had been located on other common archive websites.

(16) The Trust put in place a process to manage complaints from affected individuals.

(17) The Trust responded to a small number of local media enquiries.

Regulatory reporting obligations and consequences

Terms of reference 9

6.10. The legal requirement[5] is that the Trust should report data breaches which meet the relevant statutory threshold within 72 hours of becoming aware of it. If that deadline is missed the response should be accompanied by reasons for the delay. Although there was a slight initial delay in identifying the incident (as it was contained within an email to a staff member who had returned from leave), the incident was reported on 21 November within 72 hours from the email being seen on 19 November, and approximately 96 hours after there was arguably 'corporate knowledge' in terms of the email being sent to the Trust (albeit it was not actually seen and acted upon until approximately two days later).

[5] Article 33 UK GDPR

6.11. The ICO's response of 25 November to the incident report was to close the case with advice at that stage, namely:

> *"…We advise that in response to the personal data breach you continue to take reasonable steps to contain the incident. We also advise that you consider any steps you can take to mitigate the impact and support the affected individuals.*
>
> *Please check that your policies and procedures are fit for purpose. All staff who handle personal data should receive data protection training regularly and where possible this should be role-specific. If you haven't already done so, consider ensuring that you implement any steps you outlined in your breach report to help prevent a similar breach happening in the future.*
>
> *We also recommend you consider reviewing your process for disclosing information. You should have a robust process to double check that only relevant information is being disclosed. This could include implementing a process for checking for hidden cells or spreadsheets. See our guidance on disclosing documents to the public securely for more information. This guidance includes information on how do we avoid an accidental breach when personal information is hidden in spreadsheets and checklists that can be used when disclosing information in spreadsheets."*

6.12. The steps taken in response to the incident described elsewhere in this report give full effect to the ICO's advice.

6.13. The Trust's second regulatory requirement in reporting the incident is to notify the affected individuals ("data subjects") where an incident is likely to result in a high risk to the rights and freedoms of natural persons. The notification must be given

in clear and plain language and without undue delay, though no specific timeframe is prescribed. The notifications must at least:

(1) Include the name and contact details of the data protection officer or other contact point where more information can be obtained.

(2) Describe the likely consequences of the personal data breach; and

(3) Describe the measures taken or proposed to be taken by the Trust to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.14. Taken together, we consider that the Trust's notifications complied with these legal requirements.

What lessons can be learned from the way the incident was handled?

Terms of reference 10

Incident response team

6.15. The investigation heard that although no formal critical incident had been declared, the scale and severity of the situation necessitated the rapid formation of an incident response team. The Trust therefore quickly established a project team that included representatives from executive level as well as Information Governance patient experience and communications, to support the organisational response. This response team was chaired by the Chief People Officer and sometimes the Chief Executive, reflecting the seriousness of the incident and ensuring appropriate executive oversight.

6.16. The investigators heard that regular and frequent meetings were held, and there was a strong sense that responsibilities were well understood across the team. Clear distinctions were maintained between the responsibilities of each individual.

The investigators heard that to ensure robust oversight and accountability, a detailed action log was requested and subsequently developed by the Company Secretary. This facilitated clear tracking of actions, responsibilities, and progress. The Trust also recognised at an early stage the need for external expertise and engaged a specialist consultancy to support the organisational response, which was regarded as beneficial in strengthening the overall approach.

Review of previous FOI responses

6.17. The Trust also took down the link to the FOI website to carry out a check on all FOIs and spreadsheets to ensure there was no other repeat occurrence. This was done by CITS who did not identify any other data breaches within Excel disclosures that had been published. We note that some XLSX files remain on the Trust's 'disclosure log' webpage, in contravention of the various versions of the FOI SOP which says they must be in PDF. The Trust should remove them to reflect the SOP (or update the SOP).

Brief of external support

6.18. A communications and media crisis expert consultancy assisted the Trust executive and communication team. Their work was involved in many aspects of response planning, particularly to review comms, media statements, and assisting executives in relation to staff-wide briefing calls. They reviewed key materials, including video content of the meetings, and provided constructive feedback to support the Trust's approach and improve the approach going forward. This expert input was very well received by executives who worked with the consultancy.

The Trust wrote to approximately 5000 current staff and 3000 former staff to tell them about and apologise for the error.

6.19. The Trust's Head of Communication, and external expertise worked over the weekend of 22-23 November 2025 to prepare communications and consider the approach to the Trust's response. This began as preparing one letter, however, as it became clear that there were different levels of harm caused, and different organisations whose staff information was accessed, a decision was made to prepare variations. This developed over the following week as the Trust worked through the issue in more detail and gained a clearer understanding of its scope and those affected. As a result, the Trust adapted its communications approach, including updating its messaging, developing a set of frequently asked questions, preparing a media statement for the website, and establishing a dedicated area on the intranet.

6.20. In terms of the letters to affected individuals, the large number of the people that needed to be contacted on a personal level in a short space of time was not something the Trust had had to deal with before. A particular concern of the Trust was ensuring that correspondence was personally addressed to each individual; this required mail merge so that the letters would say *"Dear [name]"* which was not something that had been done before by the Trust. The Trust's comms team therefore had to work with IT colleagues to find a way to do that. This was an example of rapid and collaborative response where colleagues worked together and acted quickly to improve the response to the brief. It also led to a learning for the Trust going forward as it now, as a result of the breach, has this capability. As part of business continuity exercises, the Trust should continue to ensure that a range of mass staff communication scenarios are incorporated, so this knowledge and experience is not lost.

6.21. A further challenge experienced was that the Trust tried to send out the communications all at once and this was blocked by the IT systems, so they had to be sent in batches of around 100. The investigation heard that staff were surprised that the Trust hadn't ever sent (personalised) communications to staff on this scale before, but we anticipate that most such communications are typically

delivered through systems built for routine mass communications (e.g. payroll) rather than the bespoke communications that was needed here.

6.22. Because of these issues, and because of the extensive information that was coming out about the situation, there was a period of approximately 10 days between the Trust finding out about the breach and starting to notify those affected. The investigation heard that this was difficult for those dealing with the incident during this period, in terms of “holding this knowledge without being able to communicate with staff”. However, the importance of ensuring that the letters were right and communications were drafted appropriately was the priority.

The PIU Lead undertook extensive data analysis to support the incident response.

6.23. On 28 November 2025, the People Information Unit was requested to undertake retrospective data sweeps across staff lists and ESR records to ensure comprehensive capture of all relevant individuals. This request was taken forward by the People Information Service Manager on 1 December 2025 on her return from leave. The Trust was able to identify contact details for those that were still at the Trust; however, as the incident involved datasets which as far back as 2018, there were a large number of individuals who had left the Trust, but who still needed to be contacted. As a result, on 1 December 2025 the PIU service manager properly concluded that reliance on current workforce data alone would significantly underrepresent the affected population. Historic staff lists were therefore obtained and incorporated to maximise identification and matching rates.

6.24. The work undertaken by the PIU service manager during this time was significant. The information was required urgently and there were various significant challenges that were encountered, particularly for pre-ESR Go Live data, where naming conventions within roster systems were inconsistent. Variations included the use of nicknames, middle names, abbreviations, or informal identifiers (e.g.

"*Rosie*" instead of "*Rosemary*"), reflecting local familiarity rather than formal record standards.

6.25. The PIU Service manager was able to collect the information in course of three days, working over 10 hours a day, and noted it was fortunate that a year previously, they had migrated services on SQL server database to allow for automated matching.

6.26. Approximately 2,000 records could not be matched through automated processes and required manual review. This involved cross-referencing roster departments with historic staff lists to establish likely matches based on contextual information, such as departmental alignment and staffing structures at the time. Through this manual reconciliation exercise, the number of unmatched records was reduced significantly, to approximately 200 cases where definitive identification could not be established. This number included CIC and agency staff as they were not on the Trust's ESR system at any point in time. Subsequent lists were collated for those external staff affected to be shared with those external providers for them to identify and contact their staff/students affected. This reduced the overall unidentifiable staff number to 51 (and those individuals might still have become aware of the incident through internal and external publicity exercises undertaken by the Trust). As mentioned above, during this process distinct categories of individuals were also identified, including agency workers and other non-standard staff groupings, which further informed the classification and handling of records within the investigation.

6.27. Once the information was found, individuals affected were ranked on scale of severity of breach from "very high, high, medium and low". This coding was done by senior staff, who matched each of the sickness reasons in the spreadsheets with a severity score developed by members of the incident response team with the benefit of a clinical background. Each severity score was given a numerical value, so that in SQL the highest value could be located and that number would be marked as the severity of the breach in respect of that individual. For instance,

if a staff member had absence on three occasions due to headaches and then had been diagnosed with cancer and were on sick leave as a result, the staff member would be counted as “very high sensitivity” because of the seriousness of the cancer diagnosis, and this then had a bearing on approach to communication with them. An issue arose where some staff’s sickness reasons were listed as ‘unclassified or unidentified’. Out of an abundance of caution, these cases were listed as very high sensitivity. However, this significantly increased the number of individuals who required calls, as discussed later on. Seeking to stratify/cohort the staff members affected was a reasonable decision in light of the scale of the incident, although as is described below there was then some confusion among staff members (who did not know what category they were in) because different degrees of interaction had been planned for each cohort (i.e. whether they would be actively called by the Trust) whereas in at least one of the Teams briefings, all attendees were given the impression they would be called.

6.28. Work to categorise affected staff members continued as the call contact centre commenced work, as there was further data matching required each day due to changed addresses and changed surnames since the date of sickness recorded and latest contact information available held by the Trust. The verified and prioritised contact lists were provided to the contact centre to support outgoing and incoming calls. Individuals categorised as high and very high risk were issued letters containing a dedicated contact number, enabling them to make direct contact upon receipt. This formed the basis of the Contact Centre’s workflow, ensuring that incoming queries could be managed alongside proactive outreach.

6.29. Once the contact/call centre became operational, a controlled and centralised approach to data sharing was implemented. A restricted Teams channel was established, containing a live working file of affected individuals (sickness reasons and dates were not shared nor included in the file accessible by the Contact Centre), including high and very high cohorts with associated contact details. All contact centre staff accessed and updated this single dataset to maintain consistency. The file included a series of tracking fields capturing engagement

outcomes, including whether contact had been successfully established, whether personal details (telephone number, email address, and home address) had been verified, and whether the individual had received their notification letter. Where letters had not been received, preferences for alternative delivery methods were also recorded.

6.30. This dataset became the basis for ongoing data analytics activities. Initially, the file was reviewed daily, before transitioning to a three-day cycle. The purpose of this analysis was to identify individuals who had been successfully contacted but had not received correspondence, and to capture their preferred method of delivery. Based on this, additional distribution lists were generated and shared with the relevant team to facilitate further mail merges, either via email or physical post depending on the individuals' preference (some individuals requested both postal and email).

6.31. This process continued on a sustained basis until mid-February, with the final extraction completed on 11 February. The workload required extended working hours, including early morning and evening review sessions, to ensure timely updates. Each cycle involved detailed interrogation of the dataset to prepare subsequent mail merges and to refine the Contact Centre's working list.

Creation of a guide for staff to find their information

6.32. On 5 December the PIU Service Manager created a *"finding your sickness absence record in ESR"* file report guide that was shared with staff, so that individuals who were working at the Trust could go back and find out what information had been entered at that time, so that they knew what information would have been disclosed. How to access this was put in the Trust wide calls and was put on the Trust's intranet page. This kind of 'self-service' feature is sensible because it significantly reduces the work that is needed by the incident response

team, and allows affected individuals to understand the incident at their own pace and convenience.

6.33. People outside the organisation would have to email in and have this processed by the Trust's own staff. This is sensible from an information security perspective but then (necessarily) adds to the work for the Trust itself in responding to the incident.

MS Teams Live question and answer sessions with staff

6.34. Executive-led virtual sessions were introduced to communicate what had happened and provide staff with opportunities to ask questions and express concerns. These took place during the day and on one evening. The investigation found mixed responses to these sessions, although the investigators would observe that given the scale of the incident and number of individuals affected, using Teams as a key tool was a reasonable way of trying to maximise opportunities for the largest range of staff (who may be working different shift patterns or on different sites) to find out about the incident and to convey information in as close to real time as possible.

6.35. Senior leadership expressed confidence in the decision to hold staff briefing sessions, recognising that, while some sessions were more challenging than others, maintaining honesty and visibility was essential. They also appreciated that there also acknowledgement of the efforts of operational teams, particularly in managing difficult interactions and responding under pressure. Overall, they wanted there to be clear emphasis on transparency and openness in communications throughout the incident response.

6.36. However, while the intent behind these sessions was recognised as positive, aiming to demonstrate care, openness, and accountability, the audience perception of the success of their delivery, and their operational impact was mixed. In particular, it was noted that:

(1) There were some discrepancies identified between the information being provided on the Teams calls, in the letters and resources, and on the calls by the call centre. That being said, information sharing evolved as further details became available, and some staff members attended multiple Teams sessions to find out more as the incident unfolded. Updates were incorporated into communications on an ongoing basis, with Frequently Asked Questions (FAQs) maintained as a live document. This resource was continuously updated to reflect emerging queries and intelligence gathered through staff interactions, ensuring a consistent and accessible source of information for those involved in the response.

(2) Due to the need to implement the sessions quickly, initially presenters were selected based on availability rather than consistency or potential suitability/experience to give a credible response. The investigation heard that in hindsight, a smaller, consistent group of well-briefed and confident presenters would likely have improved the quality and consistency of messaging. Variations in delivery style and responses may have contributed to differences in how sessions were received, with some perceived as more challenging or confrontational. In particular, reflections were that the early sessions were (or allowed for feedback which was) angry or unfairly critical of the information governance team, members of which were present at that time. Those presenting asked for feedback from communications specialists on their approach.

(3) There was also feedback regarding perceptions of executive availability. Instances where senior leaders left sessions early due to competing commitments were seen negatively, with some participants interpreting this as a lack of prioritisation. It was recognised that a more measured approach, allowing sufficient time and focus for these engagements, may have improved both perception and effectiveness.

(4) Certain Executive-led virtual sessions contributed to increased demand on the Contact Centre, with call volumes rising significantly following some events and a noticeable increase in frustration of callers. For example, the first session held on a Thursday led to a notably high volume of calls on the following day.

(5) Further issues were noted regarding session structure and facilitation. High volumes of questions submitted via chat made it difficult to manage discussions effectively, with many questions going unanswered. The investigators also heard that some comments / questions made by staff in the chat could be quite personal and targeted at those they considered should be 'attributed blame'. A more controlled approach, such as prioritising verbal questions or using a moderated "hands-up" format, was identified as a potential opportunity for improvement, and/or using the webinar format on teams or Q&A only would be an option. Some staff members reflected that more Teams sessions, or more extended sessions, may have been beneficial.

(6) Despite these challenges, it was acknowledged that such forums served an important purpose. They allowed staff to voice concerns, particularly given the emotional impact of the incident, and reinforced the organisation's commitment to transparency. It was also noted that senior leaders sharing their own personal connection to the breach helped to build credibility and trust.

6.37. While there was some reflection on whether such open forums should have been held at all, the overall view expressed to the investigators was that they remained important. Avoiding them may have led to increased pressure elsewhere, particularly on Contact Centre and email channels, and could have undermined perceptions of transparency. The investigating team recognises the range of views on this issue, but observes that the question of how to communicate around this kind of incident does not have a perfect answer. The senior leadership team sought. to behave candidly with staff in a timely way, in line with Trust values. In a complex and large organisation, Teams provides a tool which enables a wide reach to be achieved quickly, which overall is advantageous in a dynamic and

evolving situation. However, the limitations of virtual communications should also be considered. One reflection to the investigation was that if a staff member was on a Teams call at home, they might be more isolated and this could make the experience more distressing than if they were face-to-face with colleagues. The investigators hope that this feedback may be useful if the Trust or another NHS organisation were faced with a similar situation in the future.

Email address for queries

6.38. Early in the incident response process, a dedicated email address was set up with the Information Governance team to manage communications relating to the incident, which was referenced in the notification letters.

6.39. While this was likely an appropriate step, the volume of incoming messages was significantly underestimated. The inbox was initially managed by the Information Governance team, however, the investigation heard that the number of emails received quickly became overwhelming leading to delays in responses (and in turn this may have had a knock-on effect in trust and confidence among some staff).

6.40. To address this, members of the communication team provided additional support and were granted access to the mailbox, assisting with handling enquiries over a period of approximately one to ten days.

The Contact Call Centre

6.41. The Trust set up a call centre in response to the data breach to support affected individuals, particularly those identified as having had information disclosed which was highly sensitive. This was done to make sure that people who had been impacted by this situation had a place to call and get answers to their questions.

The initial development of this proposal was done very rapidly (within hours), and one member of staff was tasked with bringing people on board and running the centre. The go-live date for the call centre was 3 December, and it was expected to run for around two weeks. It transpired this was a significant underestimate.

6.42. The call centre was operated by the clinical governance team largely independently, with staff keeping the centre active five days a week from 8am to 6pm over a period of 11 weeks, only putting the phone line to voicemail over bank holidays (i.e. Christmas and New Year). During the initial incident response the call centre staff each handled around 60-90 calls a day, with calls varying from a few minutes to potentially taking up to 25 minutes each, both incoming and outgoing calls. The call centre aimed to maintain a minimum of four staff on duty each day. The team proactively contacted individuals categorised as ‘high’ or ‘very high’ risk, whilst receiving incoming calls as well. As is described above, ‘high’ or ‘very high risk’ were people whose information was deemed particularly sensitive in terms of their absence related information. They had the potential to be the most emotionally or psychologically impacted by the disclosure and were most likely to want rapid answers.

6.43. The investigators heard that the clinical governance team were widely praised for the work that they did during the response, particularly in relation to the call centre. They regularly engaged with individuals who have experienced trauma, demonstrating strong empathy, professionalism, and communication skills. Their day-to-day roles required them to respond effectively to sensitive situations, manage complex information, and to provide clear, compassionate support. As such, at a baseline level, they were considered to be the most equipped team, without prior training or discussion to determine if they were in a psychological position to take on the task, to deliver both a rapid and structured response when required efficiently but with empathy and sensitivity.

6.44. However, the investigation heard some significant challenges that the call handlers faced along the way that are important to recognise and learn from, these included:

(1) While the majority of calls were constructive, and some people were said to have been very kind to the call handlers, there were instances where they experienced challenging behaviours from callers. These were largely expressions of anger or frustration and ended with raised voices or phones being slammed down on the handlers. The investigation also heard of incredibly difficult calls with individuals who were understandably distressed as a result of the severity of the disclosures or were in a position of danger (e.g. because of domestic abuse). The investigators heard these were particularly challenging and the team found that (without any process for the same) they needed to complete safeguarding assessments for some individuals who they considered could be in danger without any training or guidance on approach. Such occurrences of anger or distress were not infrequent, and this reflected the heightened emotions and distress experienced by callers to varying degrees due to the breach. This placed significant emotional burden on individuals working in the contact centre, who were not prepared or provided support on how to deal with those.

(2) There was a very short lead-in period and a degree of uncertainty before call handlers were formally informed that they would need to step up and run the call centre. There were indirect signs over the week prior that something would be happening, such as miscellaneous calendar holds in execs diaries and the creation of a Teams channel for an unknown purpose with ‘random’ invitees. However, there was no clear communication at that stage about what this related to, just a general sense among staff that ‘something big was coming’. The relevant staff members were told on 2 December that they would be manning the call centre, go live was 3 December 2025. This left very limited time to prepare before calls began. It also became apparent during the process that some senior members of the executive team who were themselves affected had already been contacted before the wider calling

exercise began. The staff working in the call centres had a short training session and then the calls started coming in within minutes of the team being set up. Some staff had not finished reading the pre-prepared script which had arrived only 30 minutes before the centre went live. The Trust's desire to move quickly could have been briefly tempered to ensure that staff felt as 'ready to go' as possible.

(3) Most of the call handlers only became aware that their own data had been affected by the breach while they were actively working in the call centre. In some cases, this occurred when other call handlers identified their names on call lists and let them know. This created an uncomfortable situation; the investigation heard that it was disappointing they had not been told directly prior to call centre starting, especially as others involved in the data breach response had received direct communication beforehand notifying them their information was included. It was particularly hard because those individuals found out they were affected and within minutes had to start talking/taking calls from others who were affected. Though as a general point, the investigation heard that this experience made conversations easier for callers to know that the person they were speaking to was 'in the same boat'.

(4) The investigation heard that other teams were perceived to have a 'choice' in terms of how they participated in the incident response, whereas the clinical governance team working in the call centre felt that it was an instruction. Furthermore, there was no consultation with the handlers to assess whether they were psychologically and emotionally equipped to undertake the task. In any event, irrespective of the capabilities of the clinical governance team, the investigators heard that the nature, scale and scope of the work extended well beyond, and differed fundamentally from, the duties that staff would ordinarily be expected to perform.

(5) Staff were initially told that the call centre work had to take priority, with urgent tasks and existing commitments to be put on hold. This led to cancelled meetings and, in some cases, staff having to let down families as approvals and other work could not be progressed. However, it quickly became apparent that certain other responsibilities still needed to continue, creating an

expectation that some elements of their usual workload would need to be maintained alongside the demands of the call centre. Staff noted discrepancies in terms of senior staff saying they had to stand everything else down, whilst still asking for things to be completed or for updates. Ensuring that there are appropriate resources for business-as-usual activities to continue, even if a critical/major incident is not prepared, is therefore important.

(6) Staff were required to handle calls in confidence and were instructed not to discuss the work outside of the designated group. However, no appropriate or dedicated workspace was provided to support this requirement. As a result, they were not permitted to work from their usual offices, despite those environments already being used to handle confidential conversations. Staff improvised. They had to find alternative locations, often working from home or in isolated areas within the organisation. This led to staff working in the contact centre feeling physically and professionally isolated, particularly when managing difficult or confrontational calls without immediate support from colleagues nearby. The Netcall system helped mitigate some issues by allowing calls to be made from any device, including personal phones, without displaying or disclosing the user's number. This meant staff could still carry out their roles on their personal phones without compromising personal contact details, despite the lack of designated resources.

(7) Staff received some basic, practical training, but overall support and preparation were limited. In particular, there was no guidance on how to handle difficult or emotional calls, such as dealing with anger or knowing when and how to signpost or escalate concerns. Staff were largely reliant on a single script, which left them uncertain about how to respond to more complex queries. In many cases, they had to record issues and rely on others to follow up later, rather than being able to provide reassurance or answers in the moment.

(8) The investigation heard that sometimes after the trust-wide FAQ briefings/Teams meetings, calls to the Contact Centre significantly increased and there were discrepancies in what was being told to people in those

meetings compared to elsewhere. For example, in one Teams call staff attending were told they would all receive calls, but the decision had been made that anyone attending the meetings wouldn't receive calls. This point was referenced in the staff survey feedback obtained during the investigation (see paragraph 0 onwards below).

(9) There were discrepancies in staff members being allocated severity lists, some had all "very high risk" while others all "high risk". They also had separate lists, however then found there were difficulties when receiving incoming calls, as they would have to move back to the master document. Staff working in the call centre therefore made changes to the approach to reflect these challenges along the way.

(10) There was also no coaching or preparation around handling crisis communications, despite the sensitive nature of the situation. Staff were expected to begin taking calls almost immediately, while also managing the fact that some were personally affected by the breach. This created a challenging environment, compounded by practical issues such as finding appropriate space to work. Support during calls was limited, with staff often informally listening to each other's conversations to gauge how to handle difficult situations, rather than having structured, real-time guidance available. Daily call centre team checks were attended by an executive lead, and the investigators heard that these did not always feel a psychologically safe space to properly de-brief following challenging calls.

(11) The investigation heard that while the script was helpful at the beginning, there were inaccuracies and inconsistencies that became evident as the response progressed. There were instances of contradictory details, particularly around dates, which made it difficult to provide clear and confident responses to questions. The scripts themselves were lengthy (around 15 pages) and impractical to navigate during live calls, especially when dealing with distressed or angry individuals. While they provided an initial prompt, staff quickly found they relied less on them over time.

(12) Staff from HR and organisational development were asked to support the call centre due to their prior experience with similar types of conversations. However, the investigation heard that there was a perception of a general reluctance throughout the rest of the organisation to become involved. Individuals from other teams only did short shifts or partial days, often after requests for assistance were escalated due to stress and burn-out within the clinical governance team who were managing the call centre day-to-day. Later in the response timeline, after the team had already completed approximately 4,000 calls, and a backlog of over 1,000 individuals requiring follow-up, additional support was provided by “Kernow Flex” staff. The flex staff were experienced in similar HR call centre work and contributed mainly to evening shifts (6–8pm) when operating hours were extended. Supplementary staff, including those from HR and OD, received informal training covering scripts, call logging, rota management, and reporting requirements. All staff were also required to be trained on how to use Netcall system.

(13) At the outset, the clinical governance team were instructed to receive and manage complaints relating to the incident, despite these involving staff rather than patients and therefore falling outside their usual remit. Although the team raised concerns about this, they initially complied before the position was later revised following continued challenge. By that stage, however, a number of complaints had already been received and required processing. There was no clear guidance on where these complaints should be directed, resulting in uncertainty and delay. Teams were unclear whether responsibility lay with Information Governance, HR, or another function. Complaints were passed between teams, with differing instructions given at different times, and no consistent agreement on ownership. This led to inefficiencies and confusion, with complaints being redirected multiple times. Additionally, these complaints were recorded within the complaints team’s figures despite not relating to patient experience, creating further administrative burden. Staff handling the complaints were also doing so without full context or access to information about the incident, which added to the challenge of managing them appropriately.

6.45. The call centre was stood down after approximately 11 weeks, with a decision taken to cease active operations at the end of February 2026, and transition to an answerphone facility to manage any further contact.

6.46. During interviews undertaken during the investigation, the call centre team reflected that their ability to work effectively together was a significant strength. Established relationships and familiarity meant they were able to operate smoothly under pressure; however, it was acknowledged that without this existing cohesion, the situation could have been far more challenging. Feedback from service users was very positive, particularly in relation to the compassion and empathy shown by call handlers.

E-Rostering improvements

6.47. After discovery of the incident the E-rostering lead showed significant initiative in investigating the factors that led to the information being disclosed and implementing measures to prevent a similar incident occurring in the future. Within four days of identifying the issue, they had held meetings to explore the risks associated with hidden data in documents and established a structured process within the team. During this session, the team actively tested different methods of handling data, including attempting to identify and remove hidden information and examining how documents could be manipulated through various paste functions (such as pasting as values versus other formats). This enabled them to understand how hidden links and data could persist within documents. They also considered relevant ICO guidance and other resources regarding handling of hidden data. As a result, the team developed a SOP setting out clear guidance on how information should be prepared, what data must be removed, and the correct processes for securely sharing information going forward. This was shared with the PIU Service Manager for input prior to implementation.

Investigation staff survey

6.48. As part of the investigation process, a survey was shared with all currently employed RCHT staff to provide anonymous feedback on the incident handling process. 484 staff responded. This should be considered in the context of around 8,000 staff members affected by the incident. The feedback given in the staff survey demonstrates that the dominant perception among those that responded was that the Trust handled the incident poorly once identified, with 54% of respondents selecting “Poorly”. 30% selected “Adequately”. Only 16% selected “Well” or “Very Well.”

6.49. Respondents identified some positive features of the Trust’s response. This included the fact that the incident was acknowledged, that some staff were contacted promptly, that the staff working in the Trust call centre were often professional and empathetic, and that opportunities were created to ask questions. However, respondents more frequently emphasised what they believed should have been done differently: earlier notification (albeit it is unclear whether respondents mean that the spreadsheet should have been spotted sooner after it was posted in 2023, or that once the incident had been identified in 2025, notifications should have been given quicker). Respondents also said that they would have wanted more individualised information on what had been disclosed, more consistent and personalised communication, better follow-through on promised actions (e.g. where a call had been promised), better prepared briefings supported by subject-matter experts, and more practical and emotional support for affected staff.

6.50. The survey respondents told us that email was the most commonly experienced communication method regarding the incident. Where staff experienced email-only contact, this was often associated with lower satisfaction. Personal phone contact and multi-channel communication were generally viewed more positively. Teams meetings were valued by some as a beneficial forum for updates and questions,

but were frequently criticised among survey respondents overall for poor management, inconsistent messaging and providing inadequate answers for attendees.

6.51. From the perspective of staff completing the survey, the principal lessons for the Trust are:

(1) The need for stronger FOI checking and sign-off processes (albeit that the staff who have completed the survey will be unlikely to know those processes in detail).

(2) More effective training and specialist oversight.

(3) A sense that there needs to be equal protection of staff and patient data.

(4) A more personalised and trauma-informed incident response model, and

(5) Clearer visible accountability and learning.

6.52. Common themes in free-text comments included respondents saying they had experienced emotional distress, loss of trust, concern about ongoing misuse of data, perceived inconsistency with Trust values. Unfortunately, the survey evidence indicates that overall, the respondents to it generally perceived the Trust's overall response to the incident as inadequate in empathy, consistency and reassurance, even where some specific actions were recognised as helpful.

6.53. **Recommendation:** The Trust may want to bear the feedback from this survey in mind in any future response exercise, particularly in situations where an early impression is taken by an audience that certain steps will take place, which is different to what then transpires.

6.54. As is set out above, the scale, pace and circumstances of this incident at the Trust were unique. The Trust's existing incident response processes provided a framework (with some adaptation and iteration) for the response and overall the

Trust was able to communicate information about incident to a very large number of affected current and former staff in a short timeframe, with further support available for an extended period after the incident came to light. All staff involved in the incident response that have contributed to the investigation have provided valuable and contemplative feedback on what worked well, and where the experience was less positive, with a view to ensuring that, should a similar exercise need to be undertaken in the future (whether by the Trust or other parts of the NHS) the experience from this incident is put to good use.

Summary of findings, areas for improvement and safety actions

SUMMARY OF FINDINGS

6.55. The incident arose from a chain of control failures across the FOI process rather than a single error.

6.56. The immediate cause was publication of an Excel file containing pivot-table functionality that exposed hidden, line-by-line sickness absence data about named staff. This was not in accordance with the Trust's FOI SOP. Contributory factors included:

(1) Allocation of the request to collate data to a team without the strongest workforce-data-wrangling expertise.

(2) Apparent limited awareness of pivot-table and hidden-data risks.

(3) Over-reliance (in the FOI process in force at the time) on Excel inspection tools that do not remove pivot-table source data.

and

(4) The process of converting spreadsheet material before disclosure/publication was not followed or challenged during the creation, checking or data release stage of the workflow. An intrinsic weakness in the FOI process at the time was that any conversion of material into a more secure (PDF) format was the very last step of the procedure and there was no cross-checking following that. If (as here) that step was not done, then there would be an uncontrollable disclosure of any information which was not intended for disclosure.

6.57. As a result of this, sensitive personal data was disclosed inappropriately and outside the scope of the original FOI request.

6.58. Over the last three years, the Trust has updated its FOI management processes in a way which provide additional human controls to avoid the release of similar information. The main areas for potential improvement to avoid similar incidents happening in the future are:

(1) To ensure that further organisational controls for checking spreadsheets and datasets are incorporated into the FOI SOP, in particular ensuring that the FOI response process is updated to require that data files are converted to CSV wherever possible before disclosure, and incorporating other recent elements of the ICO guidance into the Trust's FOI processes.

(2) Embedding clearer guidance on pivot tables and hidden data risks into FOI procedures, particularly for information holders, while recognising that this recommendation is also applicable to other disclosures.

(3) Maintaining the second-stage review of disclosure material.

(4) Increasing the use of SharePoint or other file-sharing mechanisms, rather than email, which allow access to disclosed data to be turned off if it is shared in error, and exploring other technical data loss prevention tools.

(5) To ensure that there is clear accountability and capability across staff working in FOI and wider data-sharing processes to identify the potential risks from large volumes of sensitive information being shared, as the nature of the incident here is unlikely to be solely FOI-specific.

(6) To explore whether additional technical controls can be put in place to guard against inadvertent loss of data under FOIA (and to limit its exposure if it is disclosed). This recommendation is applicable to wider scenarios where data loss prevention may be desirable (beyond FOIA), but the Trust will need to balance this with the general need of the Trust and stakeholders to ensure the timely and right-touch levels of security to promote the efficient exchange of information.

6.59. Once the breach was identified in November 2025, the Trust acted promptly and in good faith to remove the material, report the incident, notify affected individuals and strengthen safeguards. On the evidence reviewed, the Trust met its core reporting obligations and implemented the Information Commissioner's advice in these regards.

6.60. The Trust was able to notify a very large number of staff about the incident and did so promptly. Staff worked collegiately, with candour and at pace to try to ensure that there was assurance that incident was isolated, and that everyone was told about it as quickly and comprehensively as possible.

6.61. However, the response highlighted important lessons on aspects of preparedness (which is reflective of the unprecedented nature and scale of the incident within the Trust), including communications, business continuity, staff support and the operational burden of managing a large-scale data breach.

6.62. Affected staff described distress, loss of trust and concern about misuse of their personal information. Staff supporting the response, particularly in the contact centre and incident team, also experienced significant emotional and operational pressure, often with limited preparation, workspace or structured support.

6.63. Recommendations for the Trust in this regard are:

(1) Widening role-specific training on data handling across the organisation, not limited to the FOI context, but for all staff routinely involved in data analytics where large datasets may be shared externally or with large audiences in their work.

(2) Ensuring there is an appropriate level of support and resources for staff managing high-volume contact operations.

(3) Ensuring there are effective deputisation and knowledge-sharing arrangements so that the Trust is not over-reliant on single members of staff to coordinate or deliver key steps in incident responses.

(4) Integrating the data breach process into Emergency Planning and Resilience Response processes more generally, with incident planning factoring in data loss events as well as cyber-attacks, recalls or other large-scale staff or patient contact exercises (and to incorporate into the data breach policy the possibility that a data breach may affect large numbers of people; it seemed to the investigators that it was geared more towards smaller incidents).

(5) To ensure that (in so far as possible) that prior to going live with a recall or mass contact exercise, those that are engaged in the exercise have had sufficient time to prepare.

(6) To ensure that (as far as possible) there are appropriate practical resources available to the incident response team both in the course of the incident, even if a critical- or major incident is not prepared.

(7) To carefully consider (particularly if a critical- or major- incident is not declared) the balancing of resources which are needed for the incident response with other caseloads.

(8) Ensuring that future engagement with affected individuals in any incident continues to be timely, consistent and trauma-informed.

(9) Continuing to debrief staff involved in the incident response and to take account of feedback from affected staff to help inform any response to similar incidents in future.

6.64. The safety actions contained in the associated action plan are intended to reduce recurrence risk, strengthen assurance over appropriate disclosures, and improve resilience in future responses. Other recommendations may be found in the body of the report.

References

Legislation

- Data Protection Act 2018.
- Freedom of Information Act 2000.
- UK General Data Protection Regulation.

Guidance

- Information Commissioner's Office, *"Means of communicating information (section 11)"* *Means of communicating information (section 11) | ICO*
- Information Commissioner's Office, "*How to disclose information safely: Removing personal data from information requests and datasets"* *How to disclose information safely*
- Information Commissioner's Office, "*Advisory note to public authorities"* *Information Commissioner's Office - Advisory note to public authorities | ICO*
- Information Commissioner's Office, *"Disclosing documents to the public securely: hidden personal information and how to avoid an accidental breach"* *Disclosing documents to the public securely: hidden personal information and how to avoid an accidental breach | ICO*
- Information Commissioner's Office, *"Checklist and sign off for public authorities to use for the safe disclosure of information from Excel"* *disclosure-checklist-v1_0.docx*
- Cabinet Office, *"Freedom of Information Guidance: Communication by Spreadsheet"* Freedom of Information Guidance: Communication by Spreadsheet - GOV.UK
- Royal Cornwall Hospitals NHS Trust, *"Freedom of information Guidance for Information Holders"* *Freedom of information Guidance for Information Holders v1.docx*

Policies and Procedures:

- Royal Cornwall Hospitals NHS Trust, "*Information Use Framework Policy*", November 2022.
- Royal Cornwall Hospitals NHS Trust, *"Data Breach Policy"*, December 2023.
- Royal Cornwall Hospitals NHS Trust, *"Management of Information, Records and Data Quality Policy"*, May 2024.
- Cornwall Partnership NHS Foundation Trust and Royal Cornwall Hospitals NHS Trust, *"Acceptable Use Policy",* July 2024.
- Royal Cornwall Hospitals NHS Trust, "*Information Security Policy"*, August 2024.
- Royal Cornwall Hospitals NHS Trust, "*Information Use Framework Policy"*, October 2025.
- Royal Cornwall Hospitals NHS Trust, "*Information Use Framework Policy"*, November 2025.
- Royal Cornwall Hospitals NHS Trust, "*Standard Operating Procedures*", March 2021, v. 21.
- Royal Cornwall Hospitals NHS Trust, "*Standard Operating Procedures*", September 2023 v. 24.
- Royal Cornwall Hospitals NHS Trust, "*Standard Operating Procedures*", February 2026, v. 26.
- Royal Cornwall Hospitals NHS Trust, *"Confidentiality Audit Procedure"*, August 2024.
- Royal Cornwall Hospitals NHS Trust, *"Emergency Preparedness, Resilience and Response (EPRR) Strategy"*, January 2026.
- Royal Cornwall Hospitals NHS Trust, *"Data sharing tips, tricks and pitfalls".*

Email Correspondence and Other Documents, including:

- Email chain regarding the initial report of a data breach to the Information Governance Team, subsequently forwarded to senior management, 17 November 2025 and 19 November 2025.
- Data Security and Protection Toolkit, dated 21 November 2025, in relation to the reported incident.
- Email from the Information Governance Team concerning sending spreadsheets, 25 November 2025.
- Monday Executive Meeting regarding the FOIA breach, 25 November 2025.
- Frequently Asked Questions page set up on the Trust's intranet.
- A computer coding script developed and applied to categorise the severity of sickness information by reason.
- Royal Cornwall Hospitals NHS Trust FOI Incident Call Handler Scripts and FAQs, 01 December 2025.
- NetCall Cover Rota for staff working in the call centre.