Humber and North Yorkshire Health and Care Partnership

NHS Humber and North Yorkshire Integrated Care Board (ICB)

Agenda Item No:	17ii

Report to:	Humber and North Yorkshire Integrated Care Board
Date of Meeting:	10 January 2023
Subject:	**Information Governance Incident Report**
Director Sponsor:	Karina Ellis, Executive Director of Corporate Affairs
Author:	Hayley Gillingwater, Senior Information Governance Manager Chris Wallace, Head of Infrastructure at N3i (Author of Incident Report)

STATUS OF THE REPORT:

Approve ☐ Discuss ☐ Assurance ☐ Information ☒ A Regulatory Requirement ☐

SUMMARY OF REPORT:

The ICB must complete a Data Security and Protection Toolkit (DSPT) annual self-assessment and submit this to NHS England. Part of the requirements associated with the DSPT is the submission to the Board of:

- any ICB data incidents reported to the Information Commissioner's Office (ICO).

The enclosed report provides the necessary details in relation to a data security incident that was reported to the ICO on the 03/11/2023.

The ICO considered the details of the incident and have decided not to take any further action at this time. This was confirmed in an email on the 21/11/2023.

RECOMMENDATIONS:

Members are asked to:
i) Note the data incident reported to the Information Commissioner's Office, together with the mitigation actions that are set out in the report.

ICB STRATEGIC OBJECTIVE

Managing Today	☒
Managing Tomorrow	☒
Enabling the Effective Operation of the Organisation	☒

IMPLICATIONS

Finance	The Information Commissioners Office (ICO) reserves the right to issue fines as a result of any findings they may make against an organisation. There are no indications that the ICO intends to take such action to the incidents set out in the report.
Quality	No adverse implications identified.
HR	No adverse implications identified.
Legal / Regulatory	The ICB is regulated by the ICO as a data process.
Data Protection / IG	No adverse implications are associated with the recommendation set out in this report.
Health inequality / equality	No adverse implications are associated with the recommendation set out in this report.
Conflict of Interest Aspects	No adverse implications are associated with the recommendation set out in this report.
Sustainability	No adverse implications are associated with the recommendation set out in this report.

ASSESSED RISK:

Risks associated with data migration as detailed in the report.

Mitigations:

Importance of script testing and validation; Need for comprehensive data auditing; Proactive communication and review; Data and permission governance.

MONITORING AND ASSURANCE:

The four areas highlighted in the conclusion of the report will be discussed with N3i IT and any actions will be implemented by the Senior Information Governance Manager and the Associate Director of IT.

ENGAGEMENT:

Not applicable.

REPORT EXEMPT FROM PUBLIC DISCLOSURE No ☒ Yes ☐

If yes, please detail the specific grounds for exemption.

Humber and North Yorkshire ICB Shared Folder Permission Incident – Investigation Report and Technical Analysis

Version:	1.0
Date:	23 October 2023
Prepared by:	Chris Wallace N3i Head of IT Infrastructure

Background

On the 31 October 2023, issues were identified and reported to N3i regarding the folder permissions for the ICB Hull and East Riding Place shared folders.

The folders themselves were originally housed on the NYH domain which was set up around 10 years ago and has been managed by various IT service providers. As part of plans to modernise and reduce the cost of ownership of the primary care and ICB estate, N3i has an active project to move all users and devices to a single domain.

The project has been running for the last 3 years to move users and devices to the new domain. 70% of primary care estate has been successfully migrated by this project equating to 4,550 users and devices.

Incident details

Following engagement and comms with the ICB, N3i planned to start the migration of ICB Place users and devices to the new domain. This was planned to start on the 6th of September with six weeks of migration work planned. As part of this work the file shares used by both Places required moving to the new domain.

As per standard migration project tasks, the data was moved between domains on the 02/09/23. This required a very large amount of data to be moved between domains and new permissions applied. Due to the size of the ICB user base it was not possible to mirror the process used for primary care staff therefore the data was planned to be moved and two sets of permissions applied, one for the new domain and one for the old domain. Permissions were required for the old and new domains as staff migrations would be carried out over the course of the six weeks instead of having a single migration cut over date as is the case for primary care sites.

The initial transfer of data on the 02 September 2023 failed due to disk corruption of the original shared folders on the NYH domain. The planned migration work with users was postponed and the data transfer re-planned for the 09 September 2023.

Following the data transfer on the er-scheduled date, to move it between the relevant domains scripts were used to assign logical access permissions to the files and folders within the share. These scripts have been used successfully numerous times before within the primary care element of the project although with an addition to add permissions for the old domain as well as the new.

On the 31 October 2023 ICB staff reported that there were issues with staff having access to folders which they should not. Engineers investigated the problems and identified that the permissions were not correctly applied. Remedial work was performed at this time to review and reapply permissions to ensure known access issues were resolved.

Over 6 and 7 November 2023 a full review of permissions applied was carried out and further remedial work undertaken so that existing permissions mirrored those on the old domain.

Investigation into the root cause of the access issues found that when the scripts were used to replicate the permissions onto the files and folders it failed to do this throughout the entire folder structure. The failure was found to be due to a combination of issues. The primary issue was that permissions on the NYH domain were found to have some corruption on them. Permissions on the NYH domain were found to be a mismatch of inherited and non-inherited permissions even where inheritance was switched off on the folder, which should not be possible on a Windows file share. The scripts are not intelligent enough to understand the mix of permissions that existed which has confused the logic statements within the scripts. Due to the corrupted permissions on the NYH domain, this resulted in too many folders being allowed to inherit permissions as well as having the discrete permissions applied.

The size of the data being managed is also possibly a contributing factor in the scripts failing. As the ICB Places holds over 3.80Tb of data, the permission sets for each shared folder are very large and could have led to memory issues on the server applying them.

The relevant folders which had incorrect permissions applied were identified together with those groups of ICB staff who could have had access during the period of 7.5 weeks prior to the issue being resolved.

In summary, there were 1351 folders for Hull Place with incorrect permissions. Of these 193 were found to have permissions which were incorrectly applied but did not allow additional access to users over and above other permissions in place. The remaining 1161 folders had permission which did allow additional access to data.

For East Riding of Yorkshire Place, there were 117 folders identified with incorrect permissions applied. Of these 6 were found to have permissions which were incorrectly applied but did not allow additional access to users. The remaining 115 folders had permission which did allow additional access to data.

The ICB file shares have never had file and folder auditing enabled therefore it is not possible to report on users accessing data within these folders during the period where permissions had been incorrectly applied. There is therefore a potential data breach but no evidence to support inappropriate access to files.

Lessons learnt

While spot checks are performed following a data move, due to the size of the ICB folders it wasn't possible to review the entire folder structure. To mitigate this in the future when large data sets are moved automated reports before and after the move will be generated and automatically compared to highlight issues for investigation.

Another checking mechanism which will be introduced will be providing reports to organisations of the permissions in place following the move. This allows a third party to check and also acts as a governance review of permissions in place.

File and folder auditing will also be enabled on file shares which will provide an audit log of what users have accessed, any changes to files/folders and permission changes. This will allow reporting on what has been accessed if permissions issues occur again.

Other Issues identified

Access Permissions

A review of the existing permissions has identified that the "all staff groups" security group has been used across the ICB shared folders. This allows staff access to a large number of folders regardless of what department they work within. This may not be appropriate for data stored in some areas.

It recommended that the ICB should carry out a project to review the structure and ownership of folders following the recent organisational changes to ensure that access in place is appropriate for data held and it is clear who is responsible for specific folders.

Data Quality

The quantity of the data held by the ICB is an issue for its effective management. There is 3.80TB (3800GB) of data held which is a huge amount of work documents with some of this data being over 20 years old. Reports detailing the data usage and age of files in place are below. The ICB may wish to review its document management processes against data held to ensure organisational policies are being adhered to and the data is not held beyond its retention period.

Another area of improvement could be to run a project to have all emails within PST files migrated to the online archive within NHSmail. This has the benefit of allowing the information to be available through the web browser on multiple devices rather than just the end user's corporate device and reduces data storage locally and also the risk of data loss.

Data Highlights

<table>
<tr><td></td><td>ERY</td><td>Hull</td></tr>
<tr><td>Oldest files</td><td>10-20 Years - 19.65% - 342 GB</td><td>10-20 Years - 15.99% - 346 GB</td></tr>
<tr><td>Duplicate data</td><td>488 GB</td><td>545GB</td></tr>
<tr><td>Top 3 file types</td><td>
<table>
<tr><th>File Type</th><th>Percentage of total storage</th><th>Amount Held</th></tr>
<tr><td>PST File</td><td>20.84%</td><td>363 GB</td></tr>
<tr><td>MSG File</td><td>12.46%</td><td>217 GB</td></tr>
<tr><td>MP4 Video</td><td>8.78%</td><td>153 GB</td></tr>
</table>
</td><td>
<table>
<tr><th>File Type</th><th>Percentage of total storage</th><th>Amount Held</th></tr>
<tr><td>MP4 Video</td><td>15.28%</td><td>329 GB</td></tr>
<tr><td>MSG File</td><td>14.62%</td><td>316 GB</td></tr>
<tr><td>Chrome HTML Document</td><td>13.05%</td><td>282 GB</td></tr>
</table>
</td></tr>
<tr><td>Total space used</td><td>1.70TB</td><td>2.10TB</td></tr>
</table>

Conclusion

The incident involving the incorrect application of folder permissions to ICB shared folders presents a significant lesson in the complexities and potential risks associated with data migration and permission management in large-scale IT infrastructure projects. The series of events leading to incorrect access permissions, primarily due to script failures and pre-existing permission inconsistencies, underlines the critical need for robust checks and balances.

Key takeaways from this incident include:

1. **Importance of Script Testing and Validation:** The incident highlighted a fundamental flaw in the assumption that scripts used successfully in one part of the project (the primary care estate) would work seamlessly in the ICB. This underestimation of complexities, particularly in dealing with legacy permission structures, led to oversights.
2. **Need for Comprehensive Data Auditing:** The lack of file and folder auditing in the ICB file shares was a crucial gap, which prevented the assessment of the extent of the potential data breach.
3. **Proactive Communication and Review:** The response to the incident showed the importance of proactive communication with affected users and a timely review of applied permissions. However, it also indicated a need for regular and more rigorous checks to be in place to prevent such issues.
4. **Data and Permission Governance:** The incident calls for a more strategic approach to data and permission governance within the ICB. This includes periodic reviews of data quality, permission structures, and adherence to organisational policies and standards.