Information Governance Compliance Audit Report

Date of Audit: 29/06/2018

Date of Report: 01/08/2018

Department: Bungalow A Gorseinon- Audit of security of building

Location: Gorseinon Hospital Bungalow A

Departmental Contacts: Christine Pettifer *Assistant Site Manager* Primary Care Delivery Unit & Sarah Taylor *Lead Nurse Community Hospitals, Primary Care Delivery unit* are on site however do not store information within the building.

Medical HR, Community Nursing, Cath Lab CDs, District Nursing, Podiatry, Child Disability, Orthodontics, Heath Visiting Records & Community Care information is stored within the location.

Information Governance Board Leads: Julian Quirk, Alyson Charnock, Suzanne Holloway, Christine Morrell and Debra Rees/Helen Kemp

Auditor: Chantelle Webber *Information Governance Assurance Officer* and Claire Parsons *Information Governance Manager* were also in attendance

Audit Rating:

Audit rating	Follow up timeframe
Green- Satisfactory	No further follow up needed
Amber- Partial compliance	Further formal follow up required in 6 months
Amber- Partial compliance- Breach reported to ICO	Further formal follow up required in 4 months
Red- No compliance	Further formal follow up required in 4 months
Red- No compliance- Breach reported to ICO	**Further formal follow up required in 2 months**

Report distribution:

This report will be shared in full with the audit key contacts, IGB Leads and relevant Information Governance Managers and Head of IG.

As this breach was initiated following a breach which was reported to the ICO, this report may also be made available to the ICO for evidence and assurance purposes.

The grading will be shared with the IGB.

Due to the audit being a result of an ICO reported breach, this report will also be shared with: Hazel Robinson, Director of W&OD; Rebecca Carlton, Service Director Morriston, SDU; Hilary Dover, Director Primary and Community Services; Chris White, Interim Chief Operating Officer; Pamela Wenger, SIRO

1 Background

The Information Commissioner is responsible for enforcing and promoting compliance with the requirements of the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA), both of which came into force in May 2018.

Organisations are now legally required to provide adequate assurance with regards to compliance with data protection legislation. The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers.

ABMU has a robust information governance (IG) audit programme in place, both planned and also ad hoc following an IG incident. This Audit is taking place due to an IG breach reported to the ICO.

2 Scope of the audit

To review the arrangements in place to assess the level of compliance with the Information Governance and Information Security Policies and associated requirements of the ABMU Health Board.

This audit focus is on Bungalow A based within Gorseinon Hospital grounds which is being used as a storage area. The site is used by multiple departments for storage. As a result of this, additional audits for departments storing information here are being undertaken that will link in this audit as a whole.

Datix IDs from incidents reported:
84162
84858

Instigator for the audit:
ICO reported breach

3 Audit findings and gradings

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
1: TRAINING AND AWARENESS				
1a	Mandatory training	**Observation of Bungalow storage area only.**	N/A	N/A
1b	Staff Training Compliance	**Observation of Bungalow storage area only.**	N/A	N/A
1c/1d	Access to Information Governance / Information Security policies Knowledge of the IG Intranet location & content	**Observation of Bungalow storage area only.**	N/A	N/A
1e	Awareness of rules for access to data	**Observation of Bungalow storage area only.**	N/A	N/A
1f	Knowledge of what constitutes key identifiable patient data and key identifiable personal data	**Observation of Bungalow storage area only.**	N/A	N/A
1g	Knowledge of IGB lead as first point of contact for IG queries	**Observation of Bungalow storage area only.**	N/A	N/A
1h	Knowledge of what constitutes an IG Breach and who to go to for advice	**Observation of Bungalow storage area only.**	N/A	N/A

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
1i	Knowledge of how to report an IG incident and reporting time for IG to ICO	**Observation of Bungalow storage area only.**	N/A	N/A
2: SECURITY OF PERSONAL DATA				
2a	Storage of confidential information	**Observation** **Patient records** in paper format within cardboard storage boxes within the bungalow. Boxes and some files not marked as private and confidential. **Staff records** in paper format within cardboard storage boxes within the bungalow not marked as private and confidential. Initial investigations show that files located at the site include: • Medical HR information archived files including staff information, loose files, employee relations, EWTD & H@N • Cath Labs CDs stored approximately 100 boxes - Encryption is unknown • Community nursing records • District nurse staff leavers • Staff leavers' personal files • Continuing Care information and record files • Health visiting records	Introduce a structured filing system that is well organised and enables access to information easily should a SAR be submitted. This system should also enable accurate management of retention periods of information, which in return will provide storage space. Update the information asset register (IAR) and update regularly, in order to have the ability to access the storage of information, retention periods and information asset owners with ease. Work with the necessary stakeholders to introduce a checklist/rule to follow when storing information off site.	RED

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
		• Orthodontics were found to have used the area for storage at a later date There was no structure to the storage, there were a number of boxes piled and spread across the floor. The boxes that information are being stored within have been damaged due to the weight of the boxes above. Due to the lack of structure/organisation to the filing, ease of access is unlikely if a SAR was submitted. The unorganised storage could also prevent accurate management of retention periods. There are signs on who to contact with staff names and extension numbers on the walls of the building for certain information, however these are not up to date as some members are untraceable within the Health Board (likely to have left) and others are in new roles. This information is also not available for all information being stored. There is paint poured on the floor where records are being held which seems to have been poured by intruders. As a result of this there could be a risk of some information/files being unreadable which could result in the department not having legally admissible records if they have been compromised.		

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
2b	Knowledge of how access to confidential data is restricted	**Observation** Access to the building was via the onsite Porters. The site is in poor repair and we were informed there is known asbestos, pest infestation, lack of lighting and electricity in certain areas. There is glass throughout the site however this was caused due to the break ins. Investigation shows that measures were taken in order to make the area suitable for storage. A response from Capital Planning explained there are areas contaminated by asbestos, however providing it remained undisturbed it would be safe. Investigation shows that during previous work undertaken within the building if there was pest infestation, it would have been apparent at the time of removing old base units as these provided ideal habitat. Site security is an issue and the alarm has been tampered with enabling intruders the ability to easily switch it off. Also due to the isolated location the alarm cannot always be heard when triggered. We were informed that when police are called as a result of a break in, it can be some time before they actually arrive on site meaning intruders have usually already left. The building has been accessed by intruders breaking in through windows and doors. Inside	A positive is the key accessing the building is kept with porters, therefore there is no ease of access through the poor location of keys however the ease of access to the building through breaking boarded up windows etc is of concern. Information to be removed from the area and moved into a secure building. If the information cannot be moved then information to be marked as private and confidential and secure. Lockable cabinets to be available within the area. To prevent access if there is a further break in as a short term measure. Alarm to be replaced with a more robust secure alarm system that does not allow intruders the ability to switch off and ensures the alarm can be heard clearly by other departments in the area. Cameras to be installed outside/inside the building or at least signs be put up warning the recording of CCTV surveillance.	RED

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
		the building there were no locked cabinets all information was stored in cardboard boxes within unlocked rooms. There is a concerning issue with sufficient safe storage, as the department's key on-site contacts explained they had previously highlighted their concerns on the risk of security within the area on a number of occasions. Previous notes/information that were stored within the building were removed as there was a concern with regards to the security, however other areas have now stored information within it. Investigations suggests that measures were taken to try and make the area secure however these measures have still allowed the area to be broken into. Medical HR stated these concerns have been raised and recorded on Datix however evidence of this has not been provided to IG.	Possibly have lockable rooms within the area to increase security as a short term measure. Introduce fences around the area to improve security.	
2c	Knowledge of how to maintain security of data when taken off premises	Contact is being made with the relevant areas to identify if there is any tracked record of what is being stored at the location. Medical HR audit showed that there is a record of what is being stored within the Bungalow however this information is not on the IAR. There has been no confirmation as to whether other departments have this record.	All assets should be on the IAR to allow for adequate records management	**RED**

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
2d	Awareness of security relating to passwords	**Observation of Bungalow storage area only.**	N/A	N/A
2e	Security of screens' siting to ensure confidentiality of data can be maintained	**Observation of Bungalow storage area only.** No computers within the area.	N/A	N/A
2f	Security of unattended computers	**Observation of Bungalow storage area only.**	N/A	N/A
2g	Use of whiteboards/pin boards; do they contain inappropriate patient or staff information	**Observation of Bungalow storage area only.**	N/A	N/A
2h	Security of records e.g. on wards	**Observation of Bungalow storage area only.**	N/A	N/A
2i	Cases of misfiled patient or staff information	**Observation of Bungalow storage area only.**	N/A	N/A
3: SHARING DATA				
3a/3b	Security of patient identifiable information sent outside NHS Wales Knowledge and use of email policy, encryption, Moveit and the Portal plus mail good practice.	**Observation of Bungalow storage area only.**	N/A	N/A
3c	Security of fax machines and safe haven principles	**Observation of Bungalow storage area only.** No fax machines within the area.	N/A	N/A

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
	Location security of printers			
3d	Security of sharing data with non-NHS organisations	**Observation of Bungalow storage area only.**	N/A	N/A
3e	Knowledge of consequences of sharing patient or staff information without consent	**Observation of Bungalow storage area only.**	N/A	N/A
3f	Security of conversations which may involve sensitive data	**Observation of Bungalow storage area only.**	N/A	N/A
3g	Effectiveness of identity checks before disclosure of sensitive information Maintaining data quality	**Observation of Bungalow storage area only.**	N/A	N/A
3h	Security of data when leaving phone messages	**Observation of Bungalow storage area only.**	N/A	N/A
4: CONFIDENTIAL WASTE DISPOSAL				
4a	Storage of confidential waste prior to disposal	The building is used for storage of information prior to destruction. The building security is of concern due to break ins. The information within the building is easily accessible with information not stored in lockable	Introducing a clear and organised structure with the reason for storage and the destruction date on every box of information. Maintain this information on the IAR	**RED**

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
		cabinets and not labelled private and confidential as previously mentioned. There is also no clear separation between what is actively archived and what is for destruction. Very few storage boxes have clear dates visible for when the archived information will need to be destroyed.		
4b	Destruction of confidential waste	**Observation of Bungalow storage area only.**	N/A	N/A
4c	Knowledge of retention periods for data	Lack of information on the boxes with regards to the retention periods or destruction dates.	Retention periods to be with files to identify disposal dates easily as well as on the IAR. Within all other departmental audits, questions will be asked to clarify if there is a record of what is being stored within the area and if the retention period of the information is being managed and, if so, the process in place. Questions will also be asked around why assets have not been added to the IAR.	Unable to grade until additional information received from other audits being undertaken on all departments storing information within the area.
5: INFORMATION LEAFLETS				
5a	Information leaflets - Any information leaflets the department supplies to patients, relatives or the public	**Observation of Bungalow storage area only.**	N/A	N/A

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
	Completion of a privacy notice for the department			
5b	Any direct marketing being sent *(Newsletters, invites to events etc)*	**Observation of Bungalow storage area only.**	N/A	N/A
5c	Completion of a privacy notice for the department	**Observation of Bungalow storage area only.**	N/A	N/A
6: INFORMATION ASSET REGISTRATION				
6a	Staff awareness of the Information Asset Register	There was no information of Bungalow A being used as a storage area on the IAR.	IGB Leads to ensure that if their areas have information assets in the location they are added to the IAR asap and areas are reminded of the importance of updating the IAR regularly.	**RED**
7: DATA PROTECTION IMPACT ASSESSMENT				
7a	Knowledge of Data Protection Impact Assessment (DPIA) and when they are required	**Observation of Bungalow storage area only.**	N/A	N/A
8: CONCLUDING OBSERVATIONS AND NOTES				
8a	Any other areas audited as part of the department	Attempts by IG have been made to retrieve information on who is storing information within the building to advise them of the urgency to remove the information. Additional audits will be undertaken once all are identified.	IGB Leads to contact areas in order to ensure all departments are aware of the urgency to remove information within the building and	**RED**

Audit criteria number	Audit Criteria	Observation/Comments	Recommendation	Grading (Green, Amber or Red)
			are logging what is being stored on the IAR.	
8b	Good practice	Medical HR explained that they have logged storing data here as a risk previously but were still advised to use the area for storage. IG have asked for confirmation on the department that advised this and evidence to support the raised risk however no response has been received. IG have advised to highlight this risk further and include on the risk register if not already completed.	Clarity needs to be made in order to identify if other areas as well as Medical HR raised their concerns regarding the security of the information being stored within the location. Evidence of the raising of the risk by Medical HR also needs to be seen.	**RED**

4 Follow up audit requirements

Below is the follow up timeframe for reported breaches

Audit rating	Follow up timeframe
Green- Satisfactory	No further follow up needed
Amber- Partial compliance	Further formal follow up required in 6 months
Amber- Partial compliance- Breach reported to ICO	Further formal follow up required in 4 months
Red- No compliance	Further formal follow up required in 4 months
Red- No compliance- Breach reported to ICO	**Further formal follow up required in 2 months**

Summary/conclusion

This risk to data security has been labelled RED and the raised concerns following this observation audit will go to IGB. The ICO may also be updated and urgent action plans are to drawn up by the relevant departments storing information in the Bungalow. These must be agreed in conjunction with the relevant IGB Lead(s) and IG Department, taken forward and shared urgently. The follow-up audit will follow the proposed process, which is 2 month follow-up as the audit rating has been graded red with the breach reported to the ICO.

Actions taken by IG

As the security of patient and staff data is being compromised within the area, IG have contacted the relevant departments and services required in order to take action in removing the information stored, however full action has not currently been undertaken therefore the area remains RED.

Actions taken by Capital Planning

Investigation report from Capital Planning explained that there was no asbestos material found in the area, this report was completed by a specialist asbestos company. Capital Planning also explained that no rodent contamination was found during previous work undertaken within the building including the removal of old base units which would have releveled such creatures as they provided ideal habitat.

Actions taken by Estates

Estates have changed all the wooden panels that were on the windows and have put a 6 foot fence around the area to prevent intruders from having ease of access. Changes made to the area by estates were completed after the audit.

Actions taken by Podiatry, Child Disability, Community and District Nursing and Health Visiting

After the audit was undertaken and before this report was issued IG received confirmation from the above areas explaining all information being stored were removed from the building.

Records still to be removed

Medical HR, Cardiology and Orthodontics continue to use the area for storage against IG advice.

Thanks

Thanks to Sarah Taylor and Christine Pettifer for arranging access to the building and showing us the area.

-------End of Report--------