WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Information backup - diagnostic review

Abertawe Bro Morgannwg University Health Board

Issued: September 2013

Document reference: 495A2013

Status of report

This document has been prepared for the internal use of Abertawe Bro Morgannwg University Health Board as part of work performed in accordance with statutory functions, the Code of Audit Practice and the Statement of Responsibilities issued by the Auditor General for Wales.

No responsibility is taken by the Wales Audit Office (the Auditor General and his staff) and, where applicable, the appointed auditor in relation to any member, director, officer or other employee in their individual capacity, or to any third party.

In the event of receiving a request for information to which this document may be relevant, attention is drawn to the Code of Practice issued under section 45 of the Freedom of Information Act 2000. The section 45 Code sets out the practice in the handling of requests that is expected of public authorities, including consultation with relevant third parties. In relation to this document, the Auditor General for Wales (and, where applicable, his appointed auditor) is a relevant third party. Any enquiries regarding disclosure or re-use of this document should be sent to the Wales Audit Office at infoofficer@wao.gov.uk.

The team who delivered the work comprised Melanie Williams and Andrew Strong.

Contents

Although many of the controls we would expect to see are in place within Abertawe Bro Morgannwg University Health Board (ABMU), there are some weaknesses. In particular, changes to backup procedures are not always formally agreed and communicated, and the record kept of routine Disaster Recovery tests is incomplete. Additional controls in these areas need to be developed and implemented by the Health Board.

Summary

Introduction

1. There is increased usage and reliance on Information and Communication Technology (ICT) systems. The availability of data and resilient ICT systems play an important part in the planning and delivery of patient focused care and wider population-based health improvement or surveillance programmes. The effective backup of data and information is an essential part of this process. This audit is an important topic for NHS bodies that rely on being able to access data held within ICT systems.

2. NHS bodies should have effective arrangements in place to ensure that data are backed up on a timely basis and appropriate to its criticality. Frequently, ICT systems are managed or hosted by one NHS organisation on behalf of others, so the impact of the loss of data may be at a regional or national level. Effective backups are important for both clinical and administration systems. Backups should be capable of being easily available when needed, stored safely, and checked to ensure they are both complete and accurate. Ineffective, incomplete or inaccurate backup arrangements can have a considerable impact on NHS bodies. The consequences include:

- the potential loss of clinical information about individual patients' care;
- the potential loss of information about population health;
- a potential breach of the Data Protection Act, in particular principle number seven, which could lead to an investigation by the Information Commissioner's Office; and
- reputational damage as a result of adverse media coverage and public concern about the loss of personal information.

3. During 2011-12, we completed a review of Business Continuity/Disaster Recovery (BCDR) arrangements at the Health Board. The work examined whether the Health Board had adequate arrangements in place to provide continuity of service, in the event of an emergency, significant event or adverse conditions. We found that the Health Board was generally well prepared in terms of overall BCDR arrangements, and while some aspects could be strengthened, the Health Board was aware of these areas and is taking improvement actions.

4. Arrangements for business continuity and emergency planning rely on accurate data backups being available. This data backup diagnostic is intended to compliment the BCDR review. It has been developed to examine the risks associated with key data backup controls in light of concerns arising from a recent NHS Wales data backup incident; an ageing ICT infrastructure and network; and pressures on NHS Wales' ICT budgets.

5. This data backup diagnostic review, which was carried out in July 2013, considered the following question: 'Are the key controls in relation to data backups in place?' We did not assess arrangements at an individual divisional or departmental ICT system. Nor did we assess the operational effectiveness of data backup controls or whether these controls worked as intended.

Conclusions

6. Our main conclusion is that although many of the controls we would expect to see are in place within ABMU, there are some weaknesses. In particular, changes to backup procedures are not always formally agreed and communicated, and the record kept of routine Disaster Recovery tests is incomplete. Additional controls in these areas need to be developed and implemented by the Health Board. We reached this conclusion because:

- There is clarity about the range of IT systems in use with responsibility for data backups clearly set out. However, in common with other LHB's, the Health Board recognises that there are some electronic medical devices which are not currently captured as part of the IT systems list and backup arrangements.
- Policies and procedures for data backup are in place at ABMU and are built into their backup software and the standard operating procedures (SOP's) for each system.
- An appropriate backup regime is largely in place at the Health Board, however changes to the SOP's for each system are not currently formally signed off by the system owners, data owners or IT team.
- The backup routines and processes are monitored reasonably well at the Health Board, however currently there is no complete list of DR tests run as part of routine system maintenance (i.e. creation of test systems). Therefore it is not possible to confirm that DR tests are run regularly on all systems.

Recommendations

7. This indicates that the following recommendations need to be addressed by the Health Board:

- Changes to the SOP's including changes to the backup routines should be officially signed off to ensure all parties are aware of the changes made and agree to any new backup routines, changes in responsibilities etc.
- A formal register of the DR tests carried out as part of routine system maintenance (i.e. creation of test systems) should be created to identify any systems which are not being DR tested at least annually. These systems should then be scheduled for routine DR tests.
- A review of the medical devices not covered within the IT systems backup and recovery procedures should be undertaken. These devices also pose a potential Caldicott (data security) risk.

8. Detailed findings from our work are summarised in Appendix 1.

Appendix 1

Detailed audit findings

The following table summarises the audit findings from our diagnostic review of information backup arrangements.

Key: ✓ = *controls appear in place* , ✓ = controls appear partially in place , ✗ = controls appear not in place

The expected controls that we looked for	Controls in place (✓, ✓ or ✗)	What we found
1. The LHB knows what IT systems are in use and who has responsibility to ensure these systems are being backed up properly, in particular: • There is a clear understanding about how many administrative, clinical or surveillance systems are used. • There is clarity about who (the individual) is responsible for the information e.g. a central IM&T department or devolved management to clinical departments/divisions. • Data owners are identified for all IT systems, with clear responsibility and accountability for safeguarding the organisations information.	✓	**There is clarity about the range of IT systems in use with responsibility for data backups clearly set out. However, in common with other LHB's, the Health Board recognises that there are some electronic medical devices which are not currently captured as part of the IT systems list and backup arrangements.** • The Health Board (ABMU) has a list of their IT systems on their IM&T sharepoint site. • The list of IT systems is linked to the SOP which detail backup routines, system owners, system suppliers, data owners, support contracts, etc. These SOP's also include links to the data owners manager who would be ultimately responsible for notifying IM&T if a data owner left the organisation. • ABMU are currently in the process of adding all their systems, with full details of system and data owners, to their service desk software to speed up response times at the service desk. This would be linked to the SOP's and would save service desk staff having to look the information up on sharepoint. • ABMU acknowledge that there may be standalone databases (built by department staff) which they are not aware of. However the data on all networked machines is backed up as part of the SOP for the networked equipment (PC's, laptops, etc) and these should be captured as part of that process. • All new systems or upgrades to existing systems must comply with the ABMU enterprise server backup requirements. This ensures all systems are backed up and backups checked and varied as part of the enterprise server and backup software routines.

The expected controls that we looked for	Controls in place (✓,✟ or ✗)	What we found
• Consideration has been given to backup responsibility for national hosted or regionally hosted clinical systems which increase the importance of robust backup controls. • Consideration has been given to the assurance and reporting arrangements to the Information Governance Committee and Board that backup planning, delivery and monitoring arrangements are adequate.		• Any IM&T incidents are reported to the informatics board together with the IM&T key performance indicators (KPI's). Significant issues may be reported to the full Board if the Informatics board feel this is necessary. Routine information such as backup routines are not routinely reported to the informatics board. • ABMU rely on NWIS in terms of the national systems. The information supplied to the LHB by NWIS relating to the backup routines, DR tests, national data centre, etc. for national systems is very limited. • An area of concern raised by ABMU IT staff relates to Medical Instruments. Following a recent issue brought to their attention by medical staff, they have identified that medical instruments (hand held medical scanners etc.) which do not connect to the network or a computer but store data on DVD's or memory sticks. These medical instruments do not currently fall under the control of the IT department and they do not know how wide spread this issue is. These medical instruments and the data they hold are not currently backed up as part of the IT backup routines. This issue has been identified at other LHB's

The expected controls that we looked for	Controls in place (✓, ¶ or ×)	What we found
2. There is a backup policy for each IT system, in particular: • There are clear backup policies for all IT systems. • There are clear backup procedures established for all IT systems. • The backup approach and objectives are formally agreed with data owners or key system users for all clinical and administration systems. • IM&T risks that impact upon the delivery and provision of backups are clearly identified and managed.	✓	**Policies and procedures for data backup are in place at the Health Board and are built into their backup software and the standard operating procedures (SOP's) for each system.** • At ABMU the backup requirements and routines for all systems are written into the SOP for each system. • ABMU use Comvault software and have written the backup routines for all systems and servers into the Comvault software (i.e. it is programmed to back each system and server up as per the agreed SOP's). • The SOP's are agreed with the system and data owners. • All new systems must comply with the ABMU backup requirements to allow ABMU to use Comvault to back up all systems. • The only systems which fall outside of the normal ABMU backup regime are: – National systems (backed up and controlled by NWIS). – Managed services which are backed up by the service provider. Even in the case of managed services details of the service provider are written into the SOP as well as the contract for that service. For these two types of system/service the IM&T department are not responsible for the system or service but do, via their service desk software and/or sharepoint, know who is responsible. • All IT backup risks are raised on the IT risk register which is reported to the Informatics board. An example is the risk to the 'chemo care' system where a nightly backup was identified as being insufficient to provide adequate DR cover in the event of a system fail. This is now managed by sequel logging to a dual server to ensure adequate DR cover.

The expected controls that we looked for	Controls in place (✓, ¢ or ✗)	What we found
3. An appropriate backup regime appears to be undertaken for all IT systems, in particular: • An appropriate backup regime is regularly undertaken. • Appropriate and resilient hardware and software are used to take backups. • Access and changes to the backup schedule, location and path are appropriately authorised, controlled and managed. • Backups are stored at an appropriate and secure 'off-site' location.	¢	**An appropriate backup regime is largely in place at the Health Board, however changes to the standard operating procedures (SOP's) for each system are not currently formally signed off by the system owners, data owners or IT team.** • There are SOP's in place for all the major systems which details the backup routine for that system. • ABMU use Comvault software on an enterprise server to manage the backup routines for all systems and servers. The backup routine is then added to the Comvault software which automatically carries out the backup according to the schedule. • Comvault reports after each backup routine, and live as part of the Comvault dashboard, detailing any backup issues or failure of backup routines. Each event on these reports are investigated by the IT staff and resolved until the Comvault dashboard is clear of issues. These are investigated and cleared on a daily basis. • IT staff check backup file sizes to ensure backups have been successful on a daily basis. • Currently changes to backup routines etc. are made on the SOP's following discussions between IM&T and the system and data owners, but these are not officially signed off by either IT or the data owners. • Backups are backed up to multiple locations (backed up to all the major sites where data centres are held – three sites in total).

The expected controls that we looked for	Controls in place (✓, ₵ or ✗)	What we found
4. The completeness of backups is monitored and backup validity regularly checked, in particular: • Backup success or failure is monitored regularly i.e. daily, weekly, etc. • Software is used to manage and monitor completion of backups. • File size checks are completed. • Completeness and accuracy of backups are checked and validated regularly. • Backups are tested and information recovered to the point of data restoration. • Frequency of testing backups is appropriate to the importance of the data. • Reporting arrangements are in place in relation to escalating concerns about taking backups.	₵	**The backup routines and processes are monitored reasonably well at the Health Board, however currently there is no complete list of disaster recovery (DR) tests run as part of routine system maintenance (i.e. creation of test systems). Therefore it is not possible to confirm that DR tests are run regularly on all systems.** • The Comvault software monitors the success of the backup routines on a daily basis. • The Comvault software automatically generates a set of reports detailing any issues and the backed up file sizes at the end of each nightly backup routine. The Comvault dashboard which gives live current position on any of the backup routines can be interrogated at any time by the IT staff with access. • The IT staff investigate any issues raised and the file sizes for each backup on these reports or on the Comvault dashboard daily and clear each issue. • There is currently no DR test schedule for all systems. • Most systems are DR tested whenever a test system is created as these are routinely created from the system backup. Additionally there are requests from departments for data recovery of deleted files which are partial DR tests. • A DR test is carried out whenever a system is moved to a new or virtual server; when there is a significant upgrade or system change or when there are changes to the backup routine. • Any major issues identified by Comvault or any recurring issues are reported as part of the weekly IM&T team meetings to IM&T management – add hoc reporting to IM&T management of issues also takes place if the issue is urgent. They will then escalate to the Informatics board if required.

Source: Wales Audit Office

WALES AUDIT OFFICE

SWYDDFA ARCHWILIO CYMRU

Wales Audit Office
24 Cathedral Road
Cardiff CF11 9LJ

Tel: 029 2032 0500
Fax: 029 2032 0600
Textphone: 029 2032 0660

E-mail: info@wao.gov.uk
Website: www.wao.gov.uk

Swyddfa Archwilio Cymru
24 Heol y Gadeirlan
Caerdydd CF11 9LJ

Ffôn: 029 2032 0500
Ffacs: 029 2032 0600
Ffôn Testun: 029 2032 0660

E-bost: info@wao.gov.uk
Gwefan: www.wao.gov.uk