Mastercall Healthcare

Data protection audit report

Information Commissioner's Office

Auditors:	Lee Taylor Maria Dominey
Data controller contacts:	Vicki Reynolds Mel Buck
Distribution:	Vicki Reynolds Mel Buck
Date issued:	18 January 2013

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Mastercall Healthcare.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 Mastercall Healthcare (MCH) has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 An introductory telephone call was held on 12 November 2012 with representatives of MCH to identify and agree the scope of the audit.

2. Scope of the audit

2.1 Following pre-audit discussions with MCH, it was agreed that the audit would focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and MCH with an independent assurance of the extent to which MCH, within the scope of this agreed audit is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
High assurance	The arrangements for data protection compliance with regard to governance and controls provide a high assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to reduce the risk of non-compliance. We have made two high assurance assessments and a limited number of recommendations which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report, along with management responses.

4. Summary of audit findings

4.1 Areas of good practice

An effective management structure exists in MCH for compliance with data protection legislation. Key roles include a SIRO, deputy SIRO and a Caldicott Guardian who provide leadership, oversight and support to an IG Lead and an IG Officer. Information Asset Owners (IAOs) and supporting Information Asset Administrators (IAAs) are also in place.

Data protection training is mandatory for all staff within MCH and there is a good level of awareness. The primary learning tool is the NHS online e-learning modules. Completion of this training is monitored by the IG Lead and IG Officer, and figures are reported to the IG Committee at every meeting.

Key roles such as the SIRO and IAOs have also been provided with specialised training delivered by accredited training providers.

4.2 Areas for improvement

MCH have recently implemented a risk management process across the organisation which includes the management of information risks. Further work is needed to embed information risk management and standardise the recording of risk on a new system.

MCH are in the process of updating their policies using a Care Quality Commission (CQC) approved template. Some policies are currently not correctly version-controlled and some are overdue for review.

5. Audit approach

5.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

5.2 The audit field work was undertaken at Stockport Headquarters on 29 November and Trafford Health Centre on 30 November 2012.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed findings and action plan

Scope a: Data protection governance. The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the DPA resulting in regulatory action and/or reputational damage.

a1. An appropriate set of data protection-related policies is in place at MCH, which includes an overarching Information Governance (IG) Framework setting out how MCH will manage information.

a2. The policies include a specific Data Protection Policy, an IG Policy, a Confidentiality Policy and an Information Security Policy. Policies are drafted by the key IG staff, as subject matter experts, with input from the IG Committee before sign-off.

a3. Most policies have an annual review cycle although some may be twice-yearly. All policies are version-controlled with a policy owner, and are signed off by the IG Committee.

a4. Some policies appear to be in draft format, with some overdue for review. Auditors were informed that MCH are in the process of converting the layout to a Care Quality Commission (CQC) approved version; however the contents will remain unchanged and all policies are live and accessible to all staff via the intranet.

Recommendation: Complete the updating of all policies to the new format so that policies are correctly version-controlled and reviewed on time when this becomes due.

Management Response: Accepted. This will be completed by March 2013 and then will be reviewed annually from the creation date of the policy or as and when needed in the interim. Melanie Buck will be the owner of this action however sign off of the policies will be needed by the IG Committee Group.

Lead Officer: Mel Buck

Timescale: by March 2013

a5. An effective management structure is in place at MCH for the oversight of data protection compliance with staff in key information governance roles which reflect sector requirements.

a6. The Managing Director has been appointed the SIRO. In addition, there is a deputy SIRO (also at Director-level) who works closely with the SIRO.

a7. A Caldicott Guardian has also been nominated whose primary role is the Medical Director. He provides oversight

and support to the IG Lead and an IG Officer (the IG Team).

a8. The IG Team work jointly together as a central resource to ensure IG and data protection compliance on a day-to-day basis within MCH. They also provide advice and support to staff regarding IG issues.

a9. Additionally, Information Asset Owners (IAOs) and supporting Information Asset Administrators (IAAs) have recently been nominated across the business at Head of Department level. The IG Lead is the IAO for the IG and IT department as her primary role is the IM & T Manager. Line managers also have specific data protection responsibilities in respect of their staff.

a10. An IG Committee has been functioning for some time within MCH and has responsibility for coordinating and overseeing the implementation of the IG work programme. The Caldicott Guardian is the chair of the Committee and meetings take place monthly.

a11. The Committee has as appropriate make up of staff from across the business including the SIRO, deputy SIRO and the IG Team. Any action points arising from discussions are allocated to nominated individuals and followed up at the next meeting.

a12. All MCH committees including the IG Committee report to the CQC Assurance Committee who report directly to the Board. The Caldicott Guardian also chairs the CQC Assurance Committee, and the SIRO and deputy SIRO also attend this group's meetings which ensures that IG issues will be communicated where required.

a13. MCH have recently implemented a risk management process across the organisation which includes the management of information risks. Work on this has been undertaken during the course of the year, and is not yet fully complete.

a14. The risk management process is supported by a documented Risk Management Strategy, Risk Policy and Procedure as well as additional guidance for staff.

a15. A Risk Management Assurance Committee (RMAC) has been established in the last year, which is chaired by a Risk Manager and attended by key IG staff including the SIRO, deputy SIRO, Caldicott Guardian and the IG Lead. The presence of IG staff provides a flow of information to and from the IG Committee in relation to potential IG related risks.

a16. The 'DAC-Risk' system has been introduced to some departments. It is designed to act as an electronic tool for the management of risk registers. The Corporate Risk Register is now on DAC-Risk although this does not currently include any information risks.

Recommendation: Transfer all registers relating to personal data to DAC-Risk and ensure that all related risks are identified, assessed and entered onto the registers.

Management Response: Accepted. This is currently in the development stages by Audit South West but we are hoping to have this up and running in the next six months. All the registers relating to personal data will be transferred onto DAC-Risk the week commencing the database being implemented. Melanie Buck will be the owner of transferring the data.

Lead Officer: Mel Buck

Timescale: by June 2013

a17. Information Asset Registers (IARs) are also relatively new to MCH. These registers will also be used to record risks to specific information assets and the IAO. Auditors were supplied with a copy of the IAR for the IG department which is currently an Excel document. It is soon to be transferred to DAC-Risk and the relevant risks entered onto it.

a18. MCH have a number of mechanisms in place to enable them to monitor their compliance with data protection policies and the effectiveness of related controls. The IG Policy documents the requirement for them to have these QA processes in place.

a19. Assurance is provided by an internal and external audit function, and an Audit Committee. External audits are carried out by 'Audit South West' and evidence was provided to show that IG matters are the subject of individual audits on occasion. This focus on IG within audit planning cycles is assisted by the appointment of the deputy SIRO as the chair of the Audit Committee.

a20. MCH carry out a monthly internal audit of calls to the medical centres, for accuracy and adherence to IG policies and procedures. 3% of calls (minimum of one call per member of staff) to both GPs and out-of-hours call handlers are audited by the Caldicott Guardian and the Call Centre Manager, as appropriate.

a21. The IG Team personally carry out a monthly check of departments to ensure a set list of physical security guidelines are also being followed (e.g. ID passes are worn, screens are locked when desks unattended, shredding bins are not overflowing, etc.).

a22. The IG Lead in her role as IM & T Manager regularly produces reports from the Adastra system used in MCH to ensure technical security rules are being adhered to, such as checks for unauthorised access to sensitive electronic personal data.

a23. In line with their role as an NHS business partner, MCH are obliged to complete parts of the NHS IG Toolkit, and this is the responsibility of the IG Team.

a24. Logs of IG training figures and information security incidents are maintained by the IG Team and the information from the logs is reported by the Team to the IG Committee at each meeting for the oversight of compliance in these areas. Each individual incident is discussed by the Committee and the risk registers updated where necessary.

a25. MCH do not carry out Privacy Impact Assessments, however they have recently established a 'Confidentiality Audit' process which is similar in that it examines the impact on individuals' expectation of confidentiality prior to the introduction of any new system or project.

a26. It was reported that three Confidentiality Audits have been conducted to date, including on the new DAC-Risk system.

a27. The process for completing the Confidentiality Audits is formally documented and the relevant IAO is responsible for the completion of a questionnaire which is then signed off by the IG Committee. The questionnaire results will continue to be reviewed on an annual basis by the IG Lead and the IAO.

Scope b: Training and awareness. The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

Risk: If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the DPA resulting in regulatory action and/or reputational damage to the organisation.

b1. The IG Lead and IG Officer are responsible for the provision of IG training for all staff in MCH. This includes developing internal training materials and ensuring that staff complete the training appropriate to their role.

b2. Line managers are also responsible for ensuring that their staff are aware of their responsibilities and have undertaken their training.

b3. The provision of IG training is a standing item on the IG Committee's agenda, and the Terms of Reference requires that the Committee ensure that this training is completed by all staff.

b4. HR staff (who have overall responsibility for all training within MCH) also have a responsibility to ensure that staff complete IG training. HR provide coaching to some roles such as call handlers, and email confirmations of individuals' training to their line managers.

b5. Data protection training is mandatory for staff. The primary learning tool is the NHS online e-learning modules (part of the IG Toolkit which MCH have signed up to) which needs to be completed by March each year. Non-completion of the IG training modules is also a disciplinary offence.

b6. The IG Team have developed a training matrix/programme to assess which of the 20 modules available are relevant to which roles. Staff are then informed which modules they are required to complete.

b7. In addition to the e-learning modules, the IG Team developed and delivered a series of IG Presentations to all staff at the end of last year. Attendance was mandatory and the content was reviewed by auditors and found to be appropriate.

b8. There is appropriate monitoring and oversight of training completion which is a standing agenda item at each meeting of the IG Committee. A report on the numbers of staff who are yet to complete the training are provided to the Committee by the IG Team at each meeting.

b9. The IG Team also maintain oversight of staff progress by the collection of printed certificates from line managers and the use of a bespoke training database which is routinely updated by line managers further to confirmation of completion from HR by email.

b10. Where necessary (for example if staff take more than 2 attempts to pass e-learning), line managers and the IG staff will provide appropriate coaching and one-to-one assistance.

b11. The Caldicott Guardian's primary role in MCH is the Medical Director and as such he is informed by the IG Team at Committee meetings of any individual medical staff who have not completed their modules. He then emails those staff directly to remind them of their obligation to do this.

b12. A number of doctors within one team had not completed any modules at the time of audit and it was acknowledged that medical staff often require more encouragement as they are not directly employed by MCH; however it was reported that the involvement of the Caldicott Guardian usually ensures that all training is completed by March as required by the IG Toolkit.

b13. Administrative staff's training is overseen by their line managers and the Practice Managers. The IG Team regularly review the training database and will in turn chase the managers to make sure that their staff are being prompted to complete the modules as a matter of priority.

b14. Annual appraisals occasionally cover the IG modules (e.g. if any modules are yet to be done, or any problems with achieving the pass mark) but they are not discussed as standard.

b15. Induction processes include IG as a standard topic to be covered by line managers to help ensure that staff are aware of their obligations from an early stage. New staff must also sign a confidentiality agreement and complete all relevant IG modules before they are granted access to personal data.

b16. Line managers direct new staff to IG policies and a copy of the previously-delivered IG presentation, which are all available on the intranet.

b17. There is an appropriate level of refresher training to keep staff up to date on their data protection obligations in the form of the NHS e-learning modules that must be completed annually as part of the requirements for the IG Toolkit. However, there is no requirement for regular refresher training documented in any internal IG policy.

Recommendation: Stipulate the need for annual refresher training in a suitable IG policy.

Management Response: Accepted. Melanie Buck will be the owner of this action and add the need for annual IG training into the Information Governance Policy and Framework. This will be added in the next month and will be signed off at the IG Committee at the next meeting scheduled for the 4th Feb 2013.

Lead Officer: Melanie Buck

Timescale: by February 2013

b18. Senior management and the IG Team complete their modules early in each year in order to set an example and encourage other staff to complete theirs as soon as possible.

b19. The modules and the associated materials are available online at all times if staff want to access them, although this is not compulsory.

b20. In addition to the standard NHS modules MCH IG staff delivered extra awareness training to all staff at the end of last year. However there are no plans to repeat that training pending the introduction of the new '111' number. As the training was well-received, this will be considered once the situation is known.

b21. The majority of specialised DP training for key roles is provided by external bodies such as Audit South West and Dilys Jones' Associates. The IG Team arrange this training and it is usually delivered onsite.

b22. Training for the SIRO and IAO roles was provided this year by these external organisations, with a further course scheduled for IAOs in December 2012.

b23. In addition to the external training, the IG Officer also created and delivered a one-off IAO Presentation to both IAOs and IAAs.

b24. There is no requirement for MCH to provide specialist training for the processing of SARs as these are usually sent to the GP or hospital directly.

b25. There is a good level of awareness amongst staff fostered by e-learning, face-to-face training and support, video resources, an IG noticeboard onsite, and regular IG emails sent to all staff.

b26. All staff interviewed onsite were able to demonstrate an awareness of the compulsory IG training and a knowledge of where to access IG policies on the intranet.

b27. In addition, staff were familiar with the role of the IG Team and that they were able to contact them for further advice or assistance if necessary.

7.1 The agreed actions will be subject to a follow up audit to establish whether they have been implemented.

7.2 Any queries regarding this report should be directed to Maria Dominey, ICO Good Practice.

7.3 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Vicki Reynolds
Mel Buck.

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months	Progress at 6 months
Include all recommendations reflecting the numbering in the report	Taken from final version	Describe the status and action taken.	Describe the status and action taken.
A4.	Recommendation accepted. This will be completed by March 2013 and then will be reviewed annually from the creation date of the policy or as and when needed in the interim. Melanie Buck will be the owner of this action however sign off of the policies will be needed by the IG Committee Group.		
A16.	Recommendation		

		accepted. This is currently in the development stages by Audit South West but we are hoping to have this up and running in the next six months. All the registers relating to personal data will be transferred onto DAC-Risk the week commencing the database being implemented. Melanie Buck will be the owner of transferring the data.
B17.		Recommendation accepted. Melanie Buck will be the owner of this action and add the need for annual IG training into the Information Governance Policy and Framework. This will be added in the next month and will be signed off at the IG Committee at the next meeting scheduled for the 4th Feb 2013.