Wirral Clinical Commissioning Group

Governing Body Meeting – A meeting in public

Tuesday 5th March 2013
1330 - 1530
Nightingale Meeting Room, Old Market House

PUBLIC AGENDA

Ref No	Time	No	Papers	
	1330	**1.**	**PRELIMINARY BUSINESS**	
GB12-13/175		**1.1**	**Apologies for Absence:** • Simon Wagener	
		1.2	**Chair's Announcements**	
		1.3	**Declarations of Interest**	
		1.4	**Comments/questions from members of the public**	
		1.5	**Minutes of previous meetings:** • **Held on 29th January 2013** • **Held on 5th February 2013**	Draft minutes of Public GB meeting 29t Draft minutes of Public GB meeting 5th
		1.6	**Matters Arising/Actions Points:** • **Held on 29th January 2013** • **Held on 5th February 2013**	Draft Actions Points from PUBLIC GBB Mee Draft Actions Points from PUBLIC GB Meet

	1345	**2.**	**ITEMS FOR APPROVAL**	
GB12-13/176		**2.1**	**IG Policies x6** **(Mark Bakewell)**	Wirral CCG GB IG Report (Including poli
	1410		**ITEMS FOR INFORMATION AND NOTING**	
GB12-13/177		**3.1**	**Finance & Performance Report** **(Mark Bakewell)**	GB M10 Finance Cover Sheet 5th Mar GB Wirral CCG Finance Report- Mont
		3.2	**Minutes for Noting** • Wirral GP Commissioning Consortium of 15th January 2013. • Wirral Health Commissioning Consortium of 16th January 2013. • Wirral Alliance Commissioning Consortium of 10th January 2013. • Approvals Committees of 16th November 2012.	WGPCC Executive Board Minutes 15 01 WHCC Executive Board Minutes 16011 WACC Executive Board Meeting -FINAI Approvals Committee Minutes 16 Novembe
	1425	**4.**	**RISK REGISTER**	
GB12-13/178		**4.1**	**Items to be included onto the Risk Register** **(All)**	Copy of RiskRegister V3-0 update 20th Fet
	1430	**5.**	**ANY OTHER BUSINESS**	
GB12-13/179				

		6.	**DATE AND TIME OF NEXT MEETING**
			The date of the next Governing Board meeting is: Thursday 21st March 2013, 1300 - 1500 Beveridge Meeting Room, Ground Floor, Old Market House Please forward apologies to: Julie.stamper@wirral.nhs.uk

Wirral Clinical Commissioning Group

Governing Body Meeting

Minutes of Public Meeting Held on

Tuesday 29th January 2013
1500 - 1600
Room 539, 5th Floor, Old Market House

Present:

Dr P Jennings (PJ)	Chairman WCCG
Dr A Mantgani (AM)	Clinical Chief Officer WCCG
Lorna Quigley (LQ)	Chief Officer WCCG
Mark Bakewell (MB)	Chief Financial Officer WCCG
Dr P Naylor (PN)	Chair WHCC
Dr S Wells (SWells)	GP Executive WHCC
Dr J Oates (JO)	Chair WGPCC
Dr M Green (MG)	Chair WACC
Iain Stewart (IS)	Chief Officer WACC
James Kay (JK)	Lay Advisor (Audit & Governance)
Simon Wagener (SW)	Lay Advisor (Patient Champion)

In attendance:

Julie Stamper (JS)	Board Support Assistant (minute taker)

Apologies:

Dr A Ali (AA)	GP Executive WGPCC
Fiona Johnstone (FJ)	Director of Public Health
Andrew Cooper (AC)	Chief Officer WGCC
Christine Campbell (CC)	Acting Chief Officer WGPCC
Graham Hodkinson (GH)	Director of Social Services
Dr A Smethurst (AS)	Secondary Care Doctor
Mr A Dalgarno (AD)	NHS CWW

REF NO	MINUTE	ACTION
1.	**PRELIMINARY BUSINESS**	
GB12-13/140	Apologies for absence were noted as above.	
GB12-13/141	**Chair's Announcements**: No announcements.	
GB12-13/142	**Declarations of Interest**: There were no declarations of interest declared.	

Signed: Chair

GB12-13/142		**Comments/questions from members of the public**: No questions from members of the public. Attended by Gill Cox, Director of CAB.	
2.	**ITEMS FOR APPROVAL**		
GB12-13/143	**2.1**	**Stroke IASS**: A tender process has been undertaken for the Stroke Communication Support Service. The Board is asked to approve the process undertaken and award a one year contract for providing the Stroke Information, Advice and Support Service to Wirral residents. The Information, Advice & Support Service provides practical help and advice for all stroke patients and their families up to 12 months post-stroke. The Board approved the process and a one year contract will be put in place from 1st March 2013 with an option to extend.	
	2.2	**Stroke CSS**: A tender process has been undertaken for the Stroke Communication Support Service. The Board is asked to approve the process undertaken and award a one year contract for providing the Stroke Information, Advice and Support Service to Wirral residents. The Communication Support Service works closely with the Speech & Language Service and provides on-going support for those with communication difficulties for up to 2 years post-stroke. The Board approved the process and a one year contract will be put in place from 1st March 2013 with an option to extend.	
GB12-13/144	**2.3**	**PCAAL**: The Board is asked to approve the process for awarding a new three year contract for Primary Care Advice, Advocacy & Liaison Service to Wirral residents. This service will provide general and specialist practical advice (including employment support and representation advice and support for Employment Support Allowance Tribunals), and advocacy. It will promote independence, support people to maintain or improve their quality of life, and prevent individuals from requiring on-going and increasing levels of support in the management of social or practical problems. The Board approved the process for this service. Therefore a 3 year contract will be put in place commencing on 1st March 2013.	
GB12-13/145	**2.4**	**Organisational Development Action Plan**: The CCG Organisational Development plan was developed following two Governing Body development sessions. The plan was approved at the Governing Body meeting in November	

Signed: Chair

		2012, with the caveat that there were a number of needs highlighted that would need to be addressed. A similar view was held by the external panel during the site visit in December, that "the plan had to demonstrate that the CCG has assessed the skills processed by the Governing Body members and has a plan to build Governing Body competencies/skills where required". With the support of the Cheshire & Merseyside Commissioning Support Unit, an Organisational Development action plan has been developed, based from the outputs and discussion points identified as part of the development framework programme. Process steps need to be taken before the end of March 2013. There is a planned Board to Board meeting with the LMC in February which will highlight any further areas of work. An appraisal system needs to be put in place and it was decided that all Chief Officers and Chairs will need to be appraised between now and end of March. LQ will circulate the Organisational Development paper electronically and will also upload to the website. To table for the next meeting on 5th February.	**LQ**
3.	**ITEMS FOR INFORMATION AND NOTING**		
GB12-13/146	No items for information or noting today.		
4.	**ANY OTHER BUSINESS**		
GB12-13/147	No other business discussed at today's meeting.		
5.	**DATE AND TIME OF NEXT MEETING**		
	The date of the next Governing Body meeting is:- Tuesday 5th February 2013, 1300-1530 Duncan Meeting Room, Old Market House. Please forward apologies to: Julie.Stamper@wirral.nhs.uk		

Signed: Chair

Wirral Clinical Commissioning Group

Governing Body Meeting

Minutes of Meeting in Public

Tuesday 5th February 2013

Duncan Meeting Room, Old Market House

Present:

Dr P Jennings (PJ)	Chairman (Designate) WCCG
Lorna Quigley (LQ)	Chief Officer WCCG
Mark Bakewell (MB)	Chief Financial Officer WCCG
Dr P Naylor (PN)	Chair WHCC
Dr S Wells (SWells)	GP Executive WHCC
Dr J Oates (JO)	Chair WGPCC
Dr M Green (MG)	Chair WACC
Dr A Ali (AA)	GP Executive WGPCC
Iain Stewart (IS)	Chief Officer WACC
Fiona Johnstone (FJ)	Director of Public Health
Andrew Cooper (AC)	Chief Officer WGCC
James Kay (JK)	Lay Advisor (Audit & Governance)
Graham Hodkinson (GH)	Director of Social Services
Dr A Smethurst (AS)	Secondary Care Doctor
Christine Campbell (CC)	Acting Chief Officer WGPCC

In attendance:

Julie Stamper (JS)	Board Support Assistant (minute taker)
Anne-Marie Harrop (AMH)	Audit Manager, MIAA
Steve Connor (SC)	Deputy Director, MIAA
Mr A Dalgarno (AD)	NHS CWW

Apologies:

Dr A Mantgani (AM)	Clinical Chief Officer WCCG
Simon Wagener (SW)	Lay Advisor (Patient Champion)

REF NO	MINUTE	
1.	**PRELIMINARY BUSINESS**	
GB12-13/153	Apologies for absence were noted as above.	
GB12-13/154	**Chair's Announcements**: No announcements.	

Signed: Chair

GB12-13/155	**Declarations of Interest**: There were no declarations of interest declared.	
GB12-13/156	**Comments/questions from members of the public**: There was one member of the public in attendance.	
GB12-13/157	**Minutes of previous meeting**: The minutes of the meeting held on 8th January were agreed as a true record with a few typos to be corrected:- Page 1: Removed "formatted" from the margin. Page 4: Under 7.3, replace Assistant with Clinical. Page 5: Appendix c, Term of office; changed from 4 years to "agreed that the term of office is until April 2014 or until the Governing Body decide otherwise. **Action Points of previous meeting held on 8th January**: • 13/122: Mr Cook has not yet had a formal response from Dr Naylor regarding his enquiry. Background work has been done. A process has been agreed that minutes and agendas will be sent out one week prior to meetings. • 13/110: FJ will email PJ regarding re-articulating previous minutes about consortia linking in with Public Health. • 13/124: There has been a presentation regarding the financial plan a recent group meeting. Agreement reached. • 13/127: LQ reported that 2 meetings have been set up recently but then cancelled. Work is continuing regarding the Learning Disabilities Task & Finish Group.	**FJ**
2.	**ITEMS FOR APPROVAL**	
GB12-13/158	**2.1** **Financial Plan**: MB presented a report to update the Governing Body on the financial planning assumptions contained with the NHS Commissioning Board planning guidance (Everyone Counts: Planning for Patients 2013/14). The financial plan includes budgeted running costs and expenditure and is reflective of the respective workforce implications in these areas. Overall, the NHS Commissioning Board has a budget of £95.6 billion to deliver the mandate set out by the UK Government. Within this overall funding, it has allocated £65.6 billion to local health economy commissioners, CCG's and local authorities. A further £25.4 billion has been allocated for the NHS CB's commissioning of specialised healthcare, primary care and military and offender services. These are being commissioned nationally for the first time to ensure increased quality of care for patients through	

Signed: Chair

		increased consistency of provision. Clinical Commissioning Groups are required to hold a contingency of at least 0.5% of revenue within their plans in order to mitigate risks within the local health economy. This is in addition to 2% ring fenced non-recurrent funds. In order for the CCG to deliver its 1% surplus of £4.45m the overall expenditure budget for 2013/14 financial year is required to be set at £461.11m (based on the resource assumptions of £465.56m including its relative share of the PCT surplus/lodgement). The month 8 (November) recurrent values are taken as a starting point with an appropriate adjustment with predicted forecast outturn values to take into account the in-year changes. A number of other planning assumptions are then applied to the revised starting point. The prescribing budget reflects local assumptions and affordability, which is an uplift of 5% (excluding new drugs) and required cost efficiencies of 4% giving a net 1% increase on the 2012/13 outturn plus an additional 1% for new drugs and growth in prescribing. Based on a 4% efficiency requirement for the CCG using its recurrent 2013/14 allocation of £445.2m, the required level of QIPP savings equates to £17.8m. Within the resources section of the paper, an adjustment has been made to the NHS Wirral CCG's allocation for specialised services £25m) that will be the remit of the relevant Area Teams of the National Commissioning Board. The CCG will need to discuss with the Area Team the plans for its non-recurrent expenditure equivalent to 2% (£8.9m) of its recurrent resource but with the return of resources from the PCT surplus/lodgement. Alongside there will be an additional resource for the CCG to commit in the 2013/14 financial year (£7.943m). The Governing Body was asked to note the updated planning assumptions regarding the overall financial budget for 2013/14 and that further updates will be required as further information is received regarding outstanding issues. A final paper will be brought to the CCG's March Governing Body for approval of budgets for the 2013/14 financial year.	MB
GB12-13/159	**2.2**	**<u>Draft Strategic Plan</u>**: LQ and MB presented to the Governing body the draft strategic plan covering for 2013-2016. It incorporates the recommendation from the recent planning guidance (Everyone Counts). The plan outlines key issues for the organisation and incorporates a developed set of detailed objectives. An engagement plan will need to be developed, with a diary of events in order for stakeholders and public to contribute to the plan.	

Signed: Chair

		PN thanked MB and LQ for their work in developing the plan. The plan was approved by the Governing Body. Consultation process to be launched.	
GB12-13/160	**2.3**	**<u>QIPP Plan</u>**: MB presented the QIPP plan for the CCG for the financial period covering 2013/14 – 2015/16. The Governing Body was asked for this to be considered in conjunction with the CCG's financial and strategic plans for the same period. It was acknowledged that further work is required to establish baselines and refine both cash releasing and cost avoidance savings to ensure delivery against the QIPP plan. Monitoring will be undertaken by the Quality, Performance & Finance Committee with the final QIPP plan submitted to the CCG's March Governing Body meeting. Due to the changes within the system, CCG's will be responsible for the final 2 years (2013/14 and 2014/15) of QIPP delivery and that beyond the current comprehensive spending review period, it is envisaged that the level of QIPP challenge shall increase. Each QIPP scheme areas (Urgent Care/Unplanned Care etc) are supported by a number of initiatives to support the delivery of the required changes. These include cash releasing which will impact on contracted activity with providers via an anticipated reduction in activity due to redesign/more effective pathways or cost avoidance, by preventing activity that would have happened if no changes had taken place. Any unidentified balances will need to be identified and reduced to minimal values in order to ensure delivery of overall QIPP target for the CCG. Currently there are a number of unidentified areas but these will be developed and will include pathway improvements. Clinicians to advise MB on this. The Governing Body is asked to note the progress made in co-ordinating the CCG QIPP schemes across the 2013/14 to 2015/16 financial years. The final QIPP report will be presented to the March Governing Body meeting for approval.	**MB**
GB12-13/161	**2.4**	**<u>Organisational Development Action Plan</u>**: LQ presented the OD action plan. The CCG Organisational Development Plan was developed following a Governing Body development session. The plan was approved at the Governing Body in November 2012, with the caveat that there were a number of needs highlighted that would need to be addressed.	

Signed: Chair

		Support has been given by the CSU in the production of this action plan, and it has attempted to address the issues identified in the development session. The Governing Body approved the Action Plan and the recommendations contained within the paper. A further board development session to be arranged in order to prioritise the actions contained within the plan	
3.		**ITEMS FOR INFORMATION AND NOTING**	
GB12-13/162	**3.1**	**Finance & Performance Report**: MB presented the finance and Performance report for NHS Wirral CCG as at the end of December (Month 9) within the 2012/13 financial year. The total budget allocated to Wirral CCG for the year is £467m from within the overall PCT baseline of £660m. Based on the federated model, a number of budgets are aligned to the Governing Body (£135m) to be managed on an economy wide basis and the remaining budgets devolved to the combined consortia (£332m). As at the end of December (Month 9) the year to date position for Wirral CCG is an overspend of £1.05m with over performance against commissioning expenditure of £1.75m offset by an under performance against running costs of £0.7m. The year to date variance position between Governing Body and the combined consortia is an overspend at divisional level of £5.86m with the Governing Body underspent by £4.81m. The overall CCG performance position in relation to NHS contracts shows an overspend at month 9 of £8.1m (previous month was £6.9m), primarily being due to over performance on the WUTH contract of £7.39m (previous month was £6.53m) At month 9, non-NHS contracts are overspent to date by £1.28m (previous month was £1.33m). The favourable movement in month is primarily due to the reported under performance in the Primary Care Mental Health contracts. Prescribing expenditure is currently providing a year to date underspend of £2.96m (previous month £1.92m). There is an under performance of those budgets managed at Governing Body level of £363k and under performance at divisional level of £2.6m. The performance position is based on 7 months actual data with 2 months estimated costs for November and December. There is a year to date underspend of £696k in relation to running costs at month 9, an adverse in month movement of £19k. This is due to the movement in under performance on the Commissioning Support Unit costs at Governing Body level of £421k (previous month £445k). Clinical backfill reported at consortia level continues	

Signed: Chair

		to underperform year to date (£297k). A review with the individual consortia leads is on-going to ensure all approved expenditure is being captured within the position. The CCG's forecast outturn position was subject to an urgent review by the leadership team following completion of the reporting process to identify potential actions that could be taken to rectify the financial over performance. This has led to the 3 consortia leads to identifiy a number of areas that could be recalled to support the forecast expenditure. The Governing Body noted the financial position as at the end of December 2012 and the actions taken.	
GB12-13/163	**3.2**	**Minutes for noting**: Wirral GPCC of 18th December – noted Wirral HCC of 19th December – noted Wirral ACC of 6th December – noted Audit & Governance of 31st October – noted Audit & Governance of 28th November – noted Approvals Committee of 16th November – these are still in draft form. Bring back after ratification.	
GB12-13/164	**3.3**	**CSU SLA**: MB presented the current SLA details with the Commissioning Support Unit (CSU) and outline key performance indicators for monitoring (still under development with the CSU). The CSU SLA is based on the National Framework and has been formally adopted. The CCG can pursue local advice as appropriate. The Governing Body was asked to highlight any areas for concern and to email comments to MB. The current SLA gives flexibility to the service lines that are being delivered. The Governing Body needs to assure itself they they are satisfied with the proposed delivery model. MB to send out SLA post meeting. A Statement of Intent needs to be signed by the CCG by the end of February. It was agreed to designate AM, LQ and MB for sign off. The Governing Body were asked to note the CSU SLA.	**ALL** **MB** **AM/LQ/ MB**
GB12-13/165	**3.4**	**Board Assurance Framework Development**: SC and AMH from MIAA were invited to the Governing Body meeting to present the Wirral CCG Assurance Framework Development. The aim of the session was to look at strategic risks, aims and assurances and to ensure these are embedded across the organisation. Due to the limited time available and importance, a further meeting	**PJ**

Signed: Chair

		will be scheduled to look at individual sections of the Assurance Framework.	
4.	**RISK REGISTER**		
GB12-13/166	**<u>Items to be included on the Risk Register</u>**: This will be updated following the risks identified in QPF and will be circulated		**JS**
5.	**ANY OTHER BUSINESS**		
	No other business.		
6.	**DATE AND TIME OF NEXT MEETING**		
	The next Governing Body meeting will be an informal meeting on:- Tuesday 19th February 2013, 1300-1500 Albert Lodge, Victoria Health Centre, Wallasey Please forward apologies to: Julie.Stamper@wirral.nhs.uk		

Signed: Chair

Wirral Clinical Commissioning Group

Governing Body Meeting

Held on Tuesday 29th January 2013

Action Points – Public Meeting

Item Number	Action Points	Responsibility	Due Date
	PUBLIC MEETING		
GB12-13/145	LQ to circulate the Organisational Development paper electronically and upload on the website.	Lorna Quigley	ASAP

Wirral Clinical Commissioning Group

Governing Body Meeting

Held on Tuesday 5th February 2013

Action Points – Meeting in Public

Item Number	Action Points	Responsibility	Due Date
	PUBLIC MEETING		
GB12-13/110	FJ to email PJ regarding re-articulation of previous minutes related to consortia linking in with Public Health.	Fiona Johnstone	March
GB12-13/158	MB to bring back a final paper to the March Governing Body for approval of budgets for the 2013/14 financial year.	Mark Bakewell	March
GB12-13/160	MB to present the final QIPP paper to the March Governing Body for approval.	Mark Bakewell	March
GB12-13/161	PJ to organise a further Board development session in order to prioritise the actions contained within the OD plan.	Philip Jennings	March
GB12-13/164	The Governing Body was asked to highlight any areas of concern regarding the CSU SLA. MB to send out the CSU SLA Statement of Intent needs to be signed by AM, LQ and MB.	All members Mark Bakewell Lorna Quigley Abhi Mantgani Mark Bakewell	ASAP ASAP 28th Feb
GB12-13/165	PJ to arrange a further date for AMH and SC from MIAA for a further Board Assurance Framework session.	Phil Jennings	February
GB12-13/166	Risk Register to be updated and circulated.	Julie Stamper	ASAP

NHS

Wirral Clinical Commissioning Group

Information Governance			
Agenda Item:	2.1	**Reference:**	GB12-13/176
Report to:	Governing Body	**Meeting Date:**	5th March
Lead Officer:	Suzanne Crutchley LL.M Information and Corporate Governance Manager CWW CSU		
Contributors:	Mark Bakewell CFO and Senior Information Risk Owner Wirral Clinical Commissioning Group		
Governance:	**Link to Commissioning Strategy**	The Information Governance Assurance Statement will be 'signed off' in March 2013, in the confidence that the Information Governance Toolkit level 2 Requirements are fully met.	
	Link to current governing body Objectives	The requirement for CCGs to use the Information Governance Toolkit was set out on 18th May 2012 in the Department of Health *Clinical Commissioning Group Authorisation: Draft guide for applicants* Specifically, Domain 4: Criteria 4.3.3, states that: *CCG has used NHS Information Governance Toolkit to assess its capability to meet information governance requirements.*	
Summary:	The purpose of this report is to update the Wirral Clinical Commissioning Group with Information Governance performance, and to demonstrate that the correct support and programmes of work are underway to meet the Information Governance Toolkit Requirements by 31st March 2013.		
Recommendation:	**To Approve**		Yes
	To Note		
	Comments	The Committee are asked to: - ask for approval from the CCG Governing Body of the policies. - commit to complete the outstanding actions, in support of the Information Governance Toolkit	
Next Steps:	The CCG and CSU will undertake to the support activities as outlined within the report.		

*This section is an assessment of the **impact** of the proposal/item. As such, it identifies the significant risks, issues and exceptions against the identified areas. Each area must contain sufficient (written in full sentences) but succinct information to allow the Board to make informed decisions. It should also make reference to the impact on the proposal/item if the Board rejects the recommended decision.*

What are the implications for the following (please state if not applicable):	
Financial	The Information Governance work area is outlined in the CSU SLA offer to the CCG. The Information and Corporate Governance Manager post is included in the CSU structure.
Value For Money	The Commissioning Support Service offer value for money through a dedicated Information and Corporate Governance Manager, who is qualified to lead on the programme of work for the CCG to achieve Information Governance compliance.
Risk	Not achieving level 2 compliance against the Information Governance Toolkit Requirements by 31st March 2013.
Legal	Meeting the requirements of the legislation which governs information, significantly the Data Protection Act 1998 and the Freedom of Information Act 2000.
Workforce	It is now a Department of Health requirement that all staff complete the NLMS ***Introduction to Information Governance*** and then the ***Information Governance: The Refresher Module*** every year thereafter. Also, that all staff meet the Information Governance code of conduct.
Equality & Human Rights	not applicable
Patient and Public Involvement (PPI)	not applicable
Partnership Working	The CCG will be working closely with the CSU, who will offer appropriate support to the CCG to become Information Governance compliant.
Performance Indicators	
Do you agree that this document can be published on the website? *(If not, please note that it may still be subject to disclosure under Freedom of Information - Freedom of Information Exemptions*	**Yes**

This section gives details not only of where the actual paper has previously been submitted and what the outcome was but also of its development path i.e. other papers that are directly related to the current paper under discussion.

Report History/Development Path				
Report Name	**Reference**	**Submitted to**	**Date**	**Brief Summary of Outcome**
IG / IT Policies		QPF	5th March 13	Approved to go to GB

Private Business

The Board may exclude the public from a meeting whenever publicity (on the item under discussion) would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted or for other special reasons stated in the resolution. If this applied, items must be submitted to the private business section of the Board (Section 1 (2) Public Bodies (Admission to Meetings) Act 1960).

The definition of "prejudicial" is where the information is of a type the publication of which may be inappropriate or damaging to an identifiable person or organisation or otherwise contrary to the public interest or which relates to the provision of legal advice (for example clinical care information or employment details of an identifiable individual or commercially confidential information relating to a private sector organisation).

If a report is deemed to be for private business, please note that the tick in the box, indicating whether it can be published on the website, must be changed to a x.

If you require any additional information please contact the Lead Director/Officer.

WIRRAL CLINICAL COMMISSIONING GROUP

QUALITY, PERFORMANCE AND FINANCE COMMITTEE

INFORMATION GOVERNANCE

PURPOSE

1. The purpose of this report is to update the Wirral Clinical Commissioning Group with Information Governance performance.

POLICES

2. The Committee is asked, in stages, to note the following policies, to reach level 1 compliance of the Information Governance Toolkit:

ICT

- Security Policy*
- Network and Infrastructure File Server Policy*
- Laptop and Portable Devices and Remote Access Policy*
- Joint Primary Care Registration Authority Policy and Procedure*

CSU

- Freedom of Information Act Policy (includes Environmental Information Regulations) (approved November)
- Subject Access Requests Policy (approved November)
- Information Governance Strategy (approved October)
- Information Governance Policy (approved October)
- Confidentiality and Data Protection Policy*
- Corporate Records Retention Policy (to include Information Lifecycle)*

For January approval

ADDITIONAL SUPPORT DOCUMENTS

3. The Committee is now asked to receive some additional documents, to reach level 2 compliance of the Toolkit:

Information Governance Induction and Annual Refresher Training Procedure

4. There will be times for some new staff to have a more 'in depth' Induction for Information Governance issues, e.g. where staff will manage patient identifiable data. Also, at times, there will be a need for some staff to have a more 'tailored' Training Needs Analysis for Information Governance issues, e.g. where there has been an information/security breach. This document

could be used in these circumstances. The document contains two appendices:

-Staff Induction Information Governance Checklist
-Staff Training Needs Analysis for Information Governance

Information Governance Spot Checks

5. Following staff training on Information Governance and the various associated Staff Briefings issued, it is important for the CCG to be assured that the training has been put in to practice. The CSU have conducted random 'spot checks' on staff across a broad sector of the CCG. The findings and recommendations are contained in a brief report.

PERFORMANCE REPORTS

6. The following are now provided on the monthly Performance Reports prepared by the CSU for the CCG:

- Information Governance incidents
- summary of the Freedom of Information requests made to the CCG
- summary of the Subject Access requests made to the CCG

STAFF E-BRIEF ARTICLES

7. All of these briefings have been prepared by the CSU. The CCG have now cascaded these to all their staff.

- IG training materials/NLMS available for all staff
- NHSmail
- Confidential waste
- Safe Haven Fax Machines
- When a Privacy Impact Assessment should be completed
- Use of the NHS Number rather than PID
- Random IG 'spot checks' to be conducted
- Smartcard induction materials and further support for staff
- The roles of the Senior Information Risk Owner and Caldicott Guardian
- Freedom of Information Act and your emails
- Process for reporting IG incidents and near-misses
- Staff feedback/lessons learnt where an IG breach/incident has occurred
- Keeping Data Flow Mapping up to date
- Fair Processing Notice (for patient/staff/contractor staff)
- IG policies approved for the CCG
- staff IG code of conduct

OUTSTANDING ACTIONS

8. The following actions need to be completed ahead of March 2013.

Staff Training

9. All staff must have completed their annual Information Governance e-learning.

10. In addition to this, the annual role specific e-learning for the Senior Information Risk Owner and the Caldicott Guardian, must be completed as well. Both post holders have completed their role specific e-learning.

IAR

11. The completed template Spreadsheet is due to be returned to Information Governance by 1st February, in order that information asset risks can be independently checked and a report prepared, by the CSU, for the Committee.

Data Flow Mapping

12. The completed template Spreadsheet is due to be returned to Information Governance by 1st February, in order that data flow risks can be independently checked and a report prepared, by the CSU, for the Committee.

Privacy Impact Assessment

13. There are currently two Privacy Impact Assessment being drafted for:
    - Care Home Assessment and Review Service
    - Long Term Conditions - risk stratification

Information Sharing Protocol

14. There are no Information Sharing Protocols currently underway.

ICO Notification

15. The annual registration with the Information Commissioner's Office (ICO), through the *Notification Process*, under the terms of the Data Protection Act 1998, must be submitted to the ICO mid/late February. The CCG as Data Controller must be registered by 1st April 2013, in order that the CCG can process Person Identifiable Data (PID).

Publication Scheme

16. There is a legal requirement under the terms of the Freedom of Information Act 2000 to produce and maintain a Publication Scheme. The ICO defines

seven classes of information that a public authority should be making available via their Publication Scheme, which are:

- **Who we are and what we do**
- **What we spend and how we spend it**
- **What our priorities are and how we are doing**
- **How we make decisions**
- **Our policies and procedures**
- **Lists and registers**
- **The services we offer**

17. As a young organisation, the CCG is not expected to hold all the information suggested in the ICO guidance for some time. However, the CCG will of course start to hold increasing amounts of information, and need to continually consider how they can proactively make this freely available, most commonly via the website.

Caldicott Guardian Notification

18. NHS and Social Care Caldicott Guardians are required to be registered on the publicly available National Register of Caldicott Guardians. The CCG must register its Caldicott Guardian by 1st April 2013.

TOOLKIT SCORES

19. A minimum of level 2 compliance for all Requirements must be reached by 31st March 2013, so that the CCG is Information Governance compliant as they enter 2013/14 as a statutory organisation.

20. Once the few outstanding actions above are completed, the Information Governance Assurance Statement can be 'signed off', the CCG will be Information Governance Toolkit compliant, and will thereby submit its scores in March 2013.

RECOMMENDATIONS

21. The Committee are asked to:
- ask for approval from the CCG Governing Body of the policies.
- commit to complete the outstanding actions, in support of the Information Governance Toolkit.

Suzanne Crutchley LL.M
Senior Governance Manager (Information Governance)
Cheshire and Merseyside Commissioning Support Unit

Cheshire and Merseyside Commissioning Support Unit
1829 Building, Countess of Chester Health Park
Liverpool Road, Chester, CH2 1HJ

ICT SECURITY POLICY

Version	**1.0**
Ratified By	**CCG Committee which includes Information Governance in the Terms of Reference**
Date Ratified	
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	
Review Date	**12 months from date of issue**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

This policy covers the following organisations:

- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group
- NHS Wirral Clinical Commissioning Group

Further information about this document:

Document name	**Cheshire ICT Service Security Strategy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Ian Hart** **Chief Operating Officer** **Telephone: 01244 650546** **Email: Ian.Hart@CheshireICT.nhs.uk**
This document should be read in conjunction with	**All other Cheshire ICT Service policies**
Published by	**Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	**Ian Hart** **Chief Operating Officer**

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

1.0 Policy Statement

This top-level information security policy should be considered as a key component of the organisation's overall information security management framework and should be considered alongside more detailed information security documentation.

2.0 Organisational Responsibilities

2.1 CCG Board

The Chief Operating Officer is responsible for this Policy.

2.2 CCG Committee which includes Information Governance in the Terms of Reference

The committee is responsible for ensuring this policy is implemented in partnership with the Cheshire ICT Service and that systems and processes are developed and monitored.

2.3 Managers

Managers and Supervisors are responsible for ensuring that all staff are aware of their responsibilities under the Policy and that it is fully implemented throughout their department.

2.4 Employees, Volunteers, Contractors, sub-contractors

All staff, whether clinical or administrative, who have access to ICT systems, have a responsibility to ensure compliance with this policy.

3.0 Planning and Implementation

3.1 This policy will be approved and ratified by the CCG Committee which includes Information Governance in the Terms of Reference

3.2 All Managers will have access to this policy via the organisation's Internet site

3.3 There are no formal training requirements for this policy although general ICT training is available via the Cheshire ICT Service

4.0 Policy

The objectives of the information security policy are to preserve:

- **Confidentiality** – Access to Data shall be confined to those with appropriate authority

- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification
- **Availability** – Information shall be available and delivered to the right person, at the time when it is needed

4.1 Management of Security

At board level, responsibility for Information Security shall reside with the Senior Information Risk Officer (SIRO).
Cheshire ICT Service's Information Security Team shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

4.2 Information Security Awareness Training

Information security awareness training should be included in the staff induction process.
An ongoing awareness programme should be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
Information security expectations of staff shall be included within appropriate job definitions.

4.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

4.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

4.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

4.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

4.8 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

4.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

4.10 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Information Security Management Group.

4.11 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the organisation's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

4.12 Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Cheshire ICT Service's Service Desk on 0844 800 9982. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.13 Classification of Sensitive Information.

The organisation shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets.
The classification **NHS Confidential** – shall be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term "NHS Confidential" shall **not** be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice. Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked NHS Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification **NHS Restricted -** shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;

- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
- NHS Restricted documents should also be stored in lockable cabinets

4.14 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Cheshire ICT Service. Users breaching this requirement may be subject to disciplinary action.

4.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the organisation before they may be used on their corporate systems. Such media must also be fully encrypted and virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

4.16 Monitoring System Access and Use

An audit trail of system access and data use by staff (where available) shall be maintained and reviewed on a regular basis.

The organisation has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

4.17 Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the SIRO before they commence operation.

4.18 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the organisation.

4.19 Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Cheshire ICT Service. Users shall not install software on the organisation's property without permission from the Cheshire ICT Service. Users breaching this requirement may be subject to disciplinary action.

4.20 Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

4.21 Reporting

The Information Security Team shall keep the SIRO informed of the information security status of the organisation by means of regular reports.

5.0 Measuring Performance

This policy will be reviewed every 12 months

The number of incidents relating to information security will be monitored and reviewed

Number of communications that raise awareness of this policy and associated issues.

6.0 Audit

Where internal audit are carrying out work that includes polices relating to Information Communications Technology or Information Governance then this policy will be audited.

7.0 Review

This policy will be reviewed 12 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.

ICT NETWORK AND INFRASTRUCTURE FILE SERVER POLICY

Version	**1.0**
Ratified By	**CCG Committee which includes Information Governance in the Terms of Reference**
Date Ratified	
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	
Review Date	**12 months from date of issue**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

This policy covers the following organisations:

- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group
- NHS Wirral Clinical Commissioning Group

Further information about this document:

Document name	**Cheshire ICT Service Network Infrastructure File Server Policy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Ian Hart** **Chief Operating Officer** **Telephone: 01244 650546** **Email: Ian.Hart@CheshireICT.nhs.uk**
This document should be read in conjunction with	**All other Cheshire ICT Service policies**
Published by	**Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	**Ian Hart** **Chief Operating Officer**

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

1.0 Introduction

This document defines the Network Infrastructure and File Server Security Policy for Clinical Commissioning Groups (CCGs)

The Network Infrastructure and File Server Security Policy applies to all business functions and information contained on the network, file servers, the physical environment and to the relevant people who support the network.

2.0 Purpose of Policy

- Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network infrastructure and file servers.
- Establishes the security responsibilities for network infrastructure and file server security.
- Provides reference to documentation relevant to this policy.

3.0 Scope of this Policy

This policy applies to all networks within Clinical Commissioning Groups used for:
:

- The storage, sharing and transmission of non-clinical and clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images
- The provision of N3 networks allowing access to the Connecting for Health Programme
- The principle assets covered by this policy can be found in each CCG Principle Systems and Assets Register

4.0 Aim

The aim of this policy is to ensure the security of Clinical Commissioning Group's networks. To do this the CCG will:

- Ensure Confidentiality
- Ensure Availability
- Ensure that the network is for users.
- Ensure that the file servers are available for the users
- Preserve Integrity
- Protect the network from unauthorised or accidental access and modification by ensuring the accuracy and completeness of the organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.
- Protect the confidentiality, availability and integrity of the network by the development of business continuity and disaster recovery plans.

5.0 The Policy

The overall Network infrastructure and File Server Security Policy for THE Clinical Commissioning Groups is described below:

The CCG information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.

To satisfy this, the CCG will undertake to the following.

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network infrastructure and File Server Security Policy in a consistent, timely and cost effective manner.

Where relevant, the CCG will comply with:

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 1998
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

The CCG will comply with other laws and legislation as appropriate.
The policy forms part of the ICT Security policy and reflects the objectives of the Information Security Management System (ISMS).

6.0 Risk Assessment

The CCG will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network infrastructure and file servers that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the network.

Formal risk assessments will be undertaken and conform to ISO17799.

7.0 Physical & Environmental Security

Network computer equipment will be housed in a controlled and secure environment.
Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.
Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers, entry and alarm controls.

The ICT Technical Team Leader is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised, or when required to do so by the ICT Security Service.
Critical or sensitive network equipment will be protected from power supply failures.

- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to secure data centre areas must be authorised by the ICT Technical Team Leader
- All visitors to data centre areas must be made aware of network security requirements.
- A log to all secure data centres must be maintained. The log will contain name, organisation, purpose of visit, date, and time in and out of all none Cheshire ICT Service staff
- All visitors to network cabinet areas must be authorised by the ICT Technical team leader.

The ICT Technical Team Leader will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted when necessary.

8.0 Access Control to Secure Network Areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The ICT Technical Team Leader will maintain and periodically review a list of those with unsupervised access.

Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- Remote access to the network will conform to the CCG Laptop and Portable Devices and Remote Access Policy.
- There must be a formal, documented user registration and de-registration procedure for access to the network.
- Departmental managers must approve user access.
- Access rights to the network will be allocated on the requirements of the user's job, rather than status.
- Security privileges (i.e. 'superuser' or network administrator rights) to the network controls will only be granted by the Technical Services Manager.
- All users to the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities Policy)
- User access rights will be immediately removed or reviewed for those users who have left the CCG, changed jobs or have been suspended.

Third Party Access Control to the Network

- Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.
- All third party access to the network must be logged.
- All third party access must be governed by NHS standards on Confidentiality and Data Protection.

- No third party can be connected unless the ICT Area Manager is satisfied that the NHS standards on Confidentiality and Data Protection have been included in the third party contract.
- Access levels for third parties will only be granted to the level required for the third parties work.
- Third party access will never be allowed Root or similar administrative rights. The third party will have their own separate account.

9.0 External Network Connections

Ensure that all connections to external networks and systems have documented and approved System Security Policies.

- Ensure that all connections to external networks and systems conform to the NHS-wide Network and File Server Security Policy, Connecting for Health Statement of Compliance and supporting guidance.
- The ICT Security Service must approve all connections to external networks and systems before they commence operation.
- Designated Home Workers can only connect to the network via Cheshire ICT Service standards and network equipment.

Maintenance Contracts
The Cheshire ICT Service will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Cheshire ICT Service Asset register.

10.0 Data and Software Exchange

Formal agreements for the exchange of data and software between organisations must be established and approved by the Information Governance Manager through an Information Sharing Protocol.

11.0 Fault Logging

The ICT Technical Team Leader is responsible for ensuring that a log of all server faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

The ICT Area Manager is responsible for ensuring that a log of all networking equipment is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

12.0 Security Operating Procedures (SyOps)

Produce Security Operating Procedures (SyOps) and security contingency plans that reflect the Network and File Server Security Policy.
Changes to operating procedures must be authorised by the ICT Security Service

13.0 Network Operating Procedures

Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation.
Changes to operating procedures must be authorised by the ICT Security Service

14.0 Data Backup and Restoration

The ICT Technical Team Leader is responsible for ensuring that backup copies of file server data are taken regularly and for backing up the network devices configuration files.

- Documented procedures for the backup process, verification and storage of backup tapes will be produced and communicated to all relevant staff.
- All backup tapes will be stored securely and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- Users are responsible for ensuring that they backup their own data to the network server.

15.0 User Responsibilities, Awareness & Training

The Cheshire ICT Service will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

- All users of the network must be made aware of the contents and implications of the Network and File Server Security Policy, Confidentiality, Data Protection and Health Care Records Policies
- Irresponsible or improper actions by users may result in disciplinary action(s).

16.0 Security Audits

The ICT Security Service will require checks on, or an audit of, actual implementations based on approved security policies.

17.0 Malicious Software

The ICT Technical Team Leader must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

Internet
The ICT Area Manager must ensure that appropriate measures are in place to monitor Internet traffic and activity.

Email
The ICT Area Manager must ensure that appropriate measures are in place to monitor Email traffic and activity

18.0 Secure Disposal or Re-use of Equipment

Ensure that where equipment is being disposed of, ICT Service Delivery staff must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten.
Where this is not possible ICT Service Delivery staff should physically destroy the disk or tape.

Ensure that where disks are to be removed from the premises for repair, where possible, the data is securely overwritten or the equipment de-gaussed by the ICT Service Delivery Team.

Where equipment is to be disposed of a certification of disposal must be supplied by the disposal company.

19.0 System Change Control

Ensure that the ICT Technical Lead reviews changes to the security of the network infrastructure.

Ensure that the ICT Technical Leader reviews changes to the security of the network servers.

All such changes must be reviewed and approved by the ICT Security Service.

- The ICT Area Manager is responsible for ensuring all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures are updated
- The ICT Security Service may require checks on, or an assessment of the actual implementation based on the proposed changes.
- The ICT Security Service is responsible for ensuring that selected hardware or software meets agreed security standards.
- As part of acceptance testing of all new network systems, the ICT Security Service will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

20.0 Security Monitoring

Ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

21.0 Reporting Security Incidents & Weaknesses

All potential security breaches must be reported to ICT Security Service.
All security incidents and weaknesses must be reported in accordance with the requirements of the Cheshire ICT Service incident reporting procedures.

22.0 Business Continuity & Disaster Recovery Plans

The ICT Area Manager must ensure that business continuity plans and disaster recovery plans are produced for the file servers and services defined in the CCG Principle Systems and Assets Registers

The ICT Area Manager must ensure that business continuity plans and disaster recovery plans are produced for the network infrastructure defined in the CCG Principle Systems and Assets Registers.

The plans must be reviewed by the ICT Security Service and tested on a regular basis.

23.0 Unattended Equipment and Clear Screen

Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

Users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time.

All workstations will have a password activated if a workstation is left unattended for a short time.

Users failing to comply will be subject to disciplinary action.

24.0 Security Responsibilities

The Cheshire ICT Service has delegated the overall security responsibility for security, policy and implementation to the ICT Security Service

25.0 Guidelines

Detailed advice on how to determine and implement an appropriate level of security is available from the ICT Security Service

26.0 Review

This policy will be reviewed 24 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.

LAPTOP AND PORTABLE DEVICES AND REMOTE ACCESS POLICY

Version	**1.0**
Ratified By	**CCG Committee which includes Information Governance in the Terms of Reference**
Date Ratified	
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	
Review Date	**12 months from date of issue**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

This policy covers the following organisations:

- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group
- NHS Wirral Clinical Commissioning Group

Further information about this document:

Document name	**Cheshire ICT Service Laptop and Portable Devices and Remote Access Policy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Ian Hart** **Chief Operating Officer** **Telephone: 01244 650546** **Email: Ian.Hart@CheshireICT.nhs.uk**
This document should be read in conjunction with	**All other Cheshire ICT Service policies**
Published by	**Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	**Ian Hart** **Chief Operating Officer**

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

1. PURPOSE

To ensure the physical and data security of portable devices owned by Clinical Commissioning Groups (CCGs) and managed and supported by the Cheshire ICT Service.
For the purpose of this policy portable devices can be defined as any equipment upon which Health Service data is held / transported.
At the date of the policy this definition would include portable devices, pen drives, Personal Data Assistants (PDAs) and mobile phones in addition to laptop and tablet Personal Computers (PCs).

2. SCOPE

This policy describes the management and use of portable devices provided by CCGs.

3. HARDWARE AND SOFTWARE

Cheshire ICT Service provides hardware and software which is compatible with CCG systems.
All appropriate hardware and software is procured and installed by the Cheshire ICT Service Delivery and users must not install additional hardware or software.
Staff with non-Cheshire ICT Service provided portable devices are not allowed to connect them to the CCG data Network.
Software downloaded from the Internet must not be loaded onto systems managed and supported by the Cheshire ICT Service.
Software obtained illegally must not be loaded onto the portable device.
Upon termination of employment or contract, the user is required to return all CCG properties as soon as possible.
The user will exercise care in using and housing CCG equipment.
The Cheshire ICT Service may recall any portable device at any time to audit its use.

4. REMOTE ACCESS

Remote access enables users to gain access to the CCG data network and other work related services. Remote access must be authenticated using an approved authentication method via a VPN token.

Only devices provided by Cheshire ICT Service will be authorised for use.
In order to be considered for remote access to the CCG data network and other work related services, approval must be given from your line manager and the Chief Operating Officer of the CCG, using the form in Appendix A. The remote access application will be managed by Cheshire ICT Service.

5. ENCRYPTED MEMORY STICKS

5.1. Allocation of Encrypted Memory Sticks

a) The allocation of an encrypted memory stick needs to be supported by:

- The budget manager against whose budget the charges will be made.
- The Manager of the service concerned.

5.2. Criteria to be met for the allocation of a Cheshire ICT Service approved encrypted memory stick

Two of the following criteria must be met for an encrypted memory stick to be allocated:

- The individual is on official business.
- The individual's post requires them to work off site.
- There is a demonstrable requirement that usage is not likely to be of an ad-hoc nature.
- When the CCG determines that the allocation of a device is needed for business continuity reasons.
- The member of staff is working in a 'flexible' capacity to complete their duties, and the risk of not meeting deadlines can be mitigated to an acceptable level through the availability of a device.
- At the discretion of the Chief Operating Officer of the CCG
- All applications for the allocation of a device must be submitted in writing by the appropriate Manager, Head of Service or Director to the Cheshire ICT Service using the attached pro-forma (see Appendix B). The application must outline the appropriate reason for the request. The budget holder must also approve the application.

a)

b) On receipt of an encrypted memory stick, the individual will be asked to sign an agreement form (see Appendix C) acknowledging receipt of the device and agreeing to abide by the instructions laid out in the Policy, or be liable for disciplinary action should the user fail to do so.

c)

d) Where a Cheshire ICT Service approved encrypted memory stick is allocated to a member of staff who is on long-term sick leave or some other prolonged absence from their duties, the manager responsible for that member of staff must consider re-allocating the device to make best use of resources and must notify the Cheshire ICT Service of the temporary transfer.

e) Where a manager suspects or believes that a Cheshire ICT Service approved encrypted memory stick is being misused, the manager responsible for that member of staff must consider withdrawing the device from the member of staff, pending an investigation to determine the facts.

5.3. Staff who are allocated a Cheshire ICT Service approved encrypted memory stick are responsible for:

- Ensuring that the Laptop and Portable Devices and Remote Access Policy is read and understood.
- Ensuring that the device is used in accordance with the Policy.
- Ensuring that if work is being carried out in public places, meeting rooms and other unprotected areas, care is taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device.
- Ensuring that the device is kept safe and secure at all times.

6. PROTECTION OF HARDWARE

The user is responsible for safeguarding of the portable device hardware. In this case, it means:

- When not in use, portable devices should be kept in a locked drawer.
- While in transit, portable devices should be in a suitable carrying case and should be kept out of view wherever possible.
- Portable device security is **your** responsibility at all times.
- Do **not** leave the portable device unattended in a public place e.g. car park.
- Do **not** keep password details in the same location as the portable device.
- Avoid leaving the portable device within sight of ground floor windows or within easy access of external doors.

7. SECURITY OF DATA

Confidential data must only be installed on portable devices which have been supplied by the Cheshire ICT Service and have an appropriate level of access security/encryption implemented.
All portable media devices that connect to the CCG data network must be encrypted. Any devices that do not meet this criteria will be blocked from use.
If work is being carried out in public places, meeting rooms and other unprotected areas care should be taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device.
Care should be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen.
Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in a disciplinary action.
A storage solution is provided centrally on the CCG data network and not on each portable device and it is the responsibility of users to utilise this.
The use of the portable device and the data on it must not be shared with family members.

8. VIRUS CONTROL

The portable device has an Anti-Virus software package installed by the Cheshire ICT Service.
This package is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files on the portable device.
CCG users must not alter the configuration of this package.
The anti-virus system's database of virus definitions **must** be updated on a regular basis, each day if possible. This means connecting the portable device to the network for the virus updates to be applied.

9. PASSWORD SECURITY

The CCG Account and Password Management Policy applies in all cases.

10. INTERNET/E-MAIL

The Internet, Email, Network and File Server Policies of the CCG are equally applicable to portable devices.

11. LOSSES AND CONFIDENTIALITY/SECURITY BREACHES

Where there is a potential for breach in patient/staff confidentiality, Reporting the loss / theft of a device to the Risk Manager on DATIX and informing the appropriate person(s) in their department as soon as possible.
Any incident should also be reported to the Cheshire ICT Service Desk.

12. ACCOUNTING/AUDIT

The software and information held on portable devices are subject to the same audit procedures as any other CCG systems.

13. LEGISLATION

Users of portable devices must comply with current legislation regarding the use and retention of patient information and use of computer systems. These include, but are not limited to:

- The Data Protection Act 1998
- Access to Health Records Act 1990
- The Copyright, Designs and Patents Act 1988

- The Computer Misuse Act 1990
- The Freedom of Information Act 2000

14. REVIEW

This policy will be reviewed 24 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.

15. APPENDICES

Appendix A – Remote Access Form
Appendix B - Request Form for Mobile Devices: Encrypted Memory Sticks
Appendix C – Agreement Form: Encrypted Memory Sticks

APPENDIX A

Remote Access Assessment Form

Name of Staff Member	Job Title	Department / Directorate

Statement of Requirements:

Questions to assist ICT assessment	Y/N	Details
Are you a lone worker?		
What proportion of time do you spend away from your base?		
Do you require access to email and or corporate information outside core hours?		
Are you a member of the CCG Emergency Planning Team?		
Do you have home broadband access?		
Do you have home dial-up access?		

ICT Recommended Solution

Laptop	VPN Token	3G	Blackberry	NHS Mail	Mobile Telephone

Head of ICT Service Development	Signature	Date

Authorisation – Yes / No

Name of Responsible Officer	Signature	Date

APPENDIX B

Request Form for Mobile Devices: Encrypted Memory Sticks

Device required and to be used by:	
Name	Position
CCG	Directorate
Email address	Telephone
Reason for requirement:	
List any other personnel who are likely to use the device: (e.g. names and designations if this is intended as a team device)	
Financial information to cover costs:	
Budget Code	Subjective Code
Name of Budget Manager	Position
Signature	Date
Authorisation:	
Name of Manager /Head of Service / Director	Position
Signature	Date

Completed forms should be returned to:

Cheshire ICT Service
1829 Building
Countess of Chester Health Park
Liverpool Road, Chester, CH2 1HJ

APPENDIX C

AGREEMENT FORM - Mobile Devices: Encrypted Memory Sticks

I agree to abide by the CCG 'Laptop and Portable Devices and Remote Access Policy', which is published on the CCG Website for information.
I agree to return the device when it is no longer needed for official CCG business.
I understand that I may be liable to disciplinary action should I fail to comply with the Policy.

Name	**Position**
Directorate	**Department**
Email address	**Telephone**
Signature	**Date**

Completed forms should be returned to:

Cheshire ICT Service
1829 Building
Countess of Chester Health Park
Liverpool Road
Chester, CH2 1HJ

Joint Primary Care Registration Authority Policy and Procedure

Version	**1.0**
Ratified By	**Wirral CCG Committee which includes Information Governance in the Terms of Reference**
Date Ratified	
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**Wirral CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	
Review Date	**12 months from date of issue**
Intended Audience	**All Wirral CCG Employees**
Impact Assessed	**Yes**

This policy covers the following organisations:

- NHS Wirral Clinical Commissioning Group

•

Further information about this document:

Document name	**Cheshire ICT Service Joint Primary Care RA Policy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Ian Hart** **Chief Operating Officer** **Telephone: 01244 650546** **Email: Ian.Hart@CheshireICT.nhs.uk**
This document should be read in conjunction with	**All other Cheshire ICT Service policies**
Published by	**Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	**Ian Hart** **Chief Operating Officer**

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

1. Scope

This policy covers the Registration Authority for organisations supported by Cheshire ICT Service including the following:

- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group
- Wirral Clinical Commissioning Group

2. Introduction

2.1 Overview

The NHS Care Records Service (NCRS) and related National Programme for Information Technology (NPfIT) services are accessed using an NCRS Smartcard. A Smartcard is a 'chip and pin' device used as a means of securely identifying a user.

For healthcare professionals to be issued with a Smartcard they must be registered through the Registration Authority. Smartcard registration and access is controlled by the Registration Authority. To register for a Smartcard, Registration Authorities are required to ask applicants for identification which satisfies the government recommended standard 'e-Gif Level 3', providing at least three forms of identification (photo and non-photo), including proof of address. Full details can be found at http://www.govtalk.gov.uk.

All National Programme for IT applications use a common security and confidentiality approach, which is also shared by various local applications. This is based on the user being assigned roles, areas of work, activities and work groups. Access is defined and authorised by the Sponsor of the user. The Sponsor would usually be the user's line manager or a senior member of staff with a direct working relationship with the user.

This document lays out the policy and procedure for Smartcard registration access control for Cheshire Information and Communication Technology (ICT) Service and its primary care stakeholder organisations.

2.2 User Identity Manager and Integrated Identity Management

User Identity Manager (UIM) is new registration software to manage NHS CRS access control and facilitate the Interface to the Electronic Staff Record (ESR). UIM uses electronic forms and digital signatures thereby removing the need for paper based workflow. The implementation of UIM requires no data to be migrated. Access control in UIM is facilitated using NHS CRS Access Control Positions (ACP) defined by the Position Based Access Control Methodology which is therefore a pre-requisite to its implementation.

Integrated Identity Management is an initiative that has been introduced by Connecting for Health to join up registration authority and human resources processes. To support this there is an option to link UIM to the Electronic Staff Record (ESR) and manage smartcard access via an ESR/UIM interface.

For Clinical Commissioning Groups it has been decided that the most effective way to manage smartcard access is currently UIM standalone.

Wirral CCG are in the process of implementing UIM, and practices currently use the pre-existing Registration Authority forms for smartcard authorisation. The UIM implementation is expected to be complete by July 2013. Until UIM completion the paper forms and processes will be used in line with the national framework.

3. Registration Authority Personnel

The Registration Authority personnel mentioned in this document and their basic responsibilities are:

- **Registration Authority Manager** – Manages the overall Registration Authority procedure in consultation with the Information Governance Teams of each stakeholder organisation. The Registration Authority Manager is responsible for setting up all policies and procedures concerning the Registration Authority. The Registration Authority Manager is responsible for meeting all requirements laid out in this document and the Registration Authorities Operational Process. The Registration Authority Manager is responsible for uploading UIM Access Positions in accordance with the processes laid out in this document.

- **Registration Authority Agent** – Registers new users, issues Smartcards, maintains and updates existing users' access. The Registration Authority Agent is responsible for carrying out Smartcard Registrations, change requests and Smartcard revocations in accordance with this document and the Registration Authorities Operational Guidance.

- **Registration Authority Sponsor** – Assigns and authorises user access, verifies user identity and unlocks Smartcards. The Sponsor is responsible for identifying new users and authorising user registrations. The Sponsor is responsible for identifying the levels of access the user will require for their role and granting authorisation to add and remove user access where necessary.

- **Smartcard Unlocker** – Can unlock smartcards and renew smartcard certificates.

- **Organisational Registration Authority Sponsor -**. The Organisational Sponsor will be the Caldicott Guardian or another board level director employed by the stakeholder organisation. This person is responsible for the overall governance of Registration Authority and Position Based Access Control arrangements.

These roles can be combined, however for certain actions where dual responsibility is required the same person cannot act as the RA Sponsor and RA Agent.

4. Registration Authority Responsibilities

- To ensure the National Registration Authority Process is adhered to in full and that any local processes are developed to support the National Registration Authority Process as outlined in the latest version of the Connecting for Health Registration Authorities Operational Guidance.

- To carry out Smartcard Registrations and Registration Authority activities in accordance with the Registration Authorities Operational Process and Guidance making sure that all

Registration Authority forms are completed correctly. This includes ensuring that all new applicants are aware of the latest NHS Care Records Service Smartcard Terms and Conditions and their responsibilities as Smartcard Users.

- To ensure that sufficient Registration Authority personnel (managers, agents and sponsors) are in place to meet the requirements of the National Registration Authority Process and the needs of the stakeholder organisations.

- To ensure that all members of the Registration Authority Team are adequately trained and familiar with local and national Registration Authority processes. This includes Registration Authority personnel keeping up to date with changes in operational guidance and the latest software and completing relevant training.

- To report incidents of misuse or anomalies to Information Security and Information Governance Managers.

- To ensure that all completed Registration Authority forms are stored securely in a locked unit and can be accessed when necessary.

- To carry out Registration Authority procedures in a timely fashion so that Users are able to access the clinical systems that they need to carry out their job.

- To ensure that Sponsors understand their responsibilities and are informed of relevant national changes. Sponsors will be familiar with the roles and activities that they are authorising and will be able to unlock Smartcards and renew certificates if necessary. Sponsor training will be implemented locally as required to meet the Registration Authority responsibilities of the organisation.

- To maintain and update user role profiles where necessary and ensure leavers user role profiles are disabled immediately their employment ceases. It will be the Sponsor's responsibility to inform the Registration Authority Team when a User leaves. The Registration Authority Team will also check monthly leavers lists provided by Human Resources and provide details of active Users to practice based Sponsors every 6 months.

- To regularly review procedures and stay up to date with national Registration Authority developments including latest software, operational guidance and its integration into Trust policies and procedures.

5. Registration Authority Processes

There are three groups of primary care smartcard users, General Practice, CCG Employed, Third Party Organisations (E.G. pharmacy, local government, independent healthcare providers). Each of these groups has a different set of processes for managing smartcards.

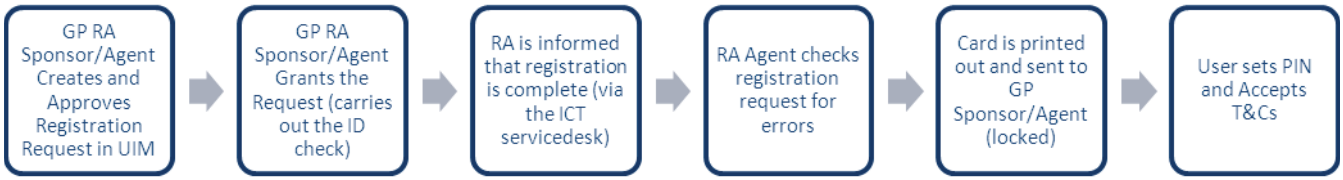
5.1 General Practice Processes

GP practices are given RA Agent status which allows the practices to carry out smartcard registrations using User Identity Manager. The practice manager identifies at least two personnel to perform the RA function. These personnel set up as both an RA Agent and an

RA Sponsor. This is so that they can either approve or grant RA requests (the same user cannot approve and grant the same request).

These processes are supported by the GP Practice Registration Authority User Guide and the RA Agent Manual.

5.1.1 GP Smartcard Registration

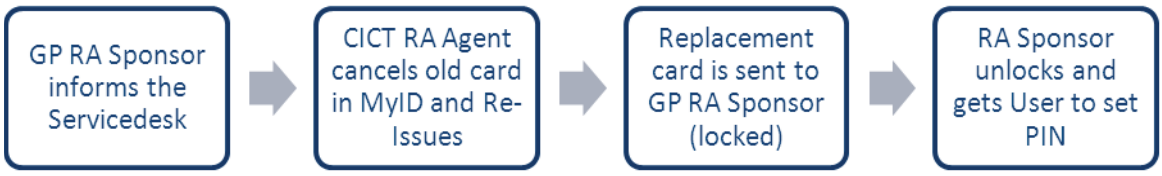


5.1.2 Adding or Removing a UIM Access Position

This process includes:

- New starters who already have a smartcard
- Leavers remaining in the NHS
- Change of Role within the practice

5.1.3 Replacing Lost/Stolen/Damaged Smartcards



If the card must be replaced urgently or there is no sponsor to unlock, then the user may visit Cheshire ICT Service to have the smartcard issued.

5.1.4 User Leaves Healthcare

5.2 General Third Party Organisation Processes

These processes cover Community Pharmacies, Local Authority, Independent Healthcare Providers and any other non GP practice or NHS organisation.

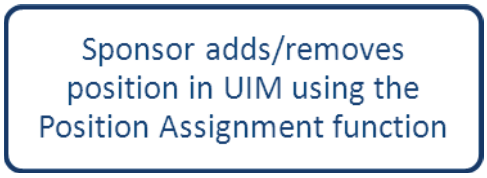
If the organisation does not have an RA Sponsor then UIM Approval will be performed by an appropriate sponsor from the CCG or Commissioning Support Organisation (usually the Information Governance Manager).

For processes relating to the transition from EPS (Electronic Prescription Service) Release 1 to EPS Release 2, refer to the Smartcard Transition Plan contained in the EPS R2 Project Documentation.

A paper based work around using RA forms will be provided by the Cheshire ICT RA Team if technical issues prevent the standard process for operating.

5.2.1 Third Party Smartcard Registration Process

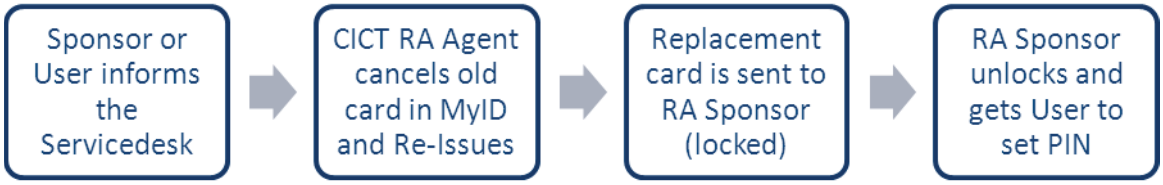
5.2.2 Adding or Removing a UIM Access Position



This process includes:

- New starters who already have a smartcard
- Leavers remaining in the NHS
- Change of Role within the practice

5.2.3 Replacing Lost/Stolen/Damaged Smartcards



If the card must be replaced urgently or there is no sponsor to unlock, then the user may visit Cheshire ICT Service to have the smartcard issued.

5.2.4 User Leaves Healthcare

5.3 Processes for Clinical Commissioning Group and Commissioning Support Unit Employed Staff

5.3.1 Smartcard Registration

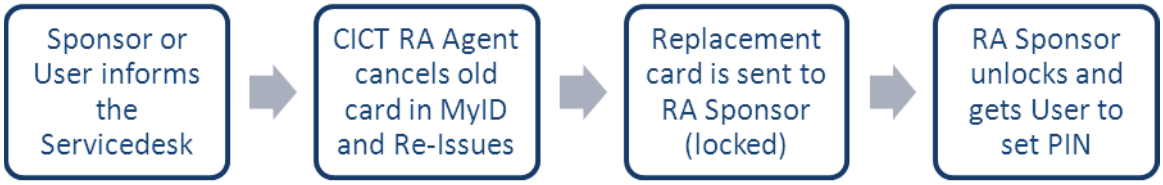
5.3.2 Adding or Removing UIM Access Position

This process includes:

- New starters who already have a smartcard
- Leavers remaining in the NHS
- Change of Role within the practice

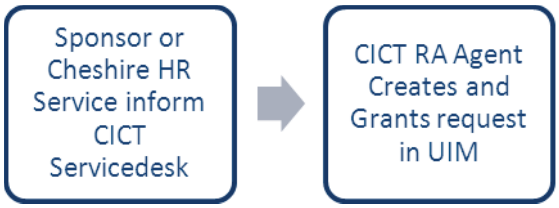
Leavers reported to Cheshire ICT Service by Cheshire HR Service will be removed via position assignment by the RA Team.

5.3.3 Replacing Lost/Stolen/Damaged Smartcards



If the card must be replaced urgently or there is no sponsor to unlock, then the user may visit Cheshire ICT Service to have the smartcard issued.

5.4.4 User Leaves Healthcare



6. Position Based Access Control (PBAC)

6.1

PBAC is the set of Access Positions that exist within User Identity Manager (UIM) which can be applied to a user's smartcard profile. Each Access Position is made up of a set of access codes which are taken from the National RBAC Database.

The PBAC is agreed locally to reflect what is required for staff groups accessing data via smartcard within an organisation.

The Registration Authority Manager is responsible for maintaining and updating the Access Positions on UIM to meet the needs of smartcard users.

6.2 Process for Tracking and Approving PBAC Changes

Includes CCGs and hosted organisations.

GP Practices

A request is raised in UIM and must be approved by the GP practice RA Sponsor / Agent.

Community Pharmacy

All community pharmacies within the CCG cluster will be offered a generic set of positions to cover their requirements for the Electronic Prescription Service (EPS) Release 2. The EPS Release 2 project board will approve these positions and any changes while the project is active. Once the project is closed this process of approval will be passed to the appropriate body.

7. Smartcard Maintenance

The Registration Authority Sponsors and GP RA Agents will carry out basic Smartcard maintenance operations including unlocking Smartcards and renewing Smartcard certificates.

When users experience problems using their Smartcard that cannot be resolved by the Sponsor they will report it to the Cheshire ICT Servicedesk. The Servicedesk Analyst will investigate the problem and escalate to the Registration Authority Team if necessary. The Registration Authority Team will then contact the user to investigate the problem.

8. Smartcard Misuse and Incident Reporting

All Smartcard users are responsible for the safety, security and use of their own Smartcard as per the terms and conditions set out in the RA01 form. In particular Smartcard users must:

- Never share their Smartcard passcode
- Never allow another user to use their Smartcard
- Never leave their Smartcard unattended unless it is stored securely
- Only access patient information that they require to carry out their role

Failure to comply with these terms and conditions will be treated as serious misconduct and dealt with through the HR disciplinary procedure.

Any member of staff must report incidents where they feel there is a risk to patient health, confidentiality or their organisation's reputation. Incidents should be reported to the Sponsor and Registration Authority Manager and the local incident reporting procedure must also be completed immediately.

9. Certificate Expiry and Renewal

Smartcard certificates are valid for two years after which the smartcard will need to be renewed. If a user attempts to log in with their smartcard and there is less than thirty days before the certificates are due to expire, the Identity Agent will notify the user that the certificates are about to expire.

The user will be given the option to self-renew, which will only work if their desktop is enabled to use the Smartcard Management System (MyID). If a software fault prevents the

user from renewing their smartcard, then it is the user's responsibility to inform a sponsor or the CICT Servicedesk that their smartcard is due to expire.

The RA Manager will provide a smartcard certificate expiry reports to appropriate personnel on request.

10. Independent Sector Healthcare Providers and Local Authorities

Cheshire ICT Service will provide Registration Authority services to Independent Sector Healthcare Providers and Local Authorities within the geographical boundaries of NHS Western Cheshire Primary Care Trust, Central and Eastern Cheshire Primary Care Trust and Warrington Primary Care Trust. This will be agreed on a case by case basis adhering to Connecting for Health Registration Authorities Operational Guidance.

Registration Authority arrangements between Cheshire ICT Service and Independent Sector Healthcare Providers or Local Authorities will be governed by an inter-organisational agreement signed by both parties (see section 16).

The Sponsor role will be assigned to a member of staff within the Independent Sector Healthcare Providers, while the Registration Authority Agent role will be performed by Cheshire ICT Service Registration Authority Team.

The operational processes for Independent Sector and Local Authority organisations are outlined in section 4.2 of this document.

11. Registration Authority Equipment

- The Registration Authority Manager will be responsible for ensuring that adequate numbers of Smartcards and working Smartcard Printers are available to meet the needs of the service.
- All Registration Authority equipment will be subject to normal Cheshire ICT Service policies and procedures governing the organisations' assets.
- Smartcard Printers will be maintained by the supplier as per the national agreement.
- The Registration Authority Manager is responsible for carrying out and documenting an Equipment Needs Assessment every six months.

12. Registration Authority Forms

Registration Authority (RA) forms will be used as a paper based fall back to User Identity Manager.

- The Registration Authority Team will ensure that completed Registration Authority and EPS forms are kept secure and confidential at all times.
- Registration Authority forms will be stored in a secure location where they can be easily accessed when necessary by authorised staff.

13. Auditing

The management and use of Smartcards will be subject to internal and external audit to ensure local and national policies are being followed. An annual internal audit will be carried out by the Cheshire ICT Service Information Security Team. This information will be reported to the Information Governance Teams of the Cheshire ICT Service stakeholder organisations.

Auditing will look to confirm that:

- All Registration Authority documents are used and stored appropriately
- Smartcards are handled securely by users
- User Role Profile amendments are performed appropriately
- Access to NPfIT Applications are controlled and managed appropriately
- Unused Smartcards are stored safely and securely

To aid in the audit process the Registration Authority Team will keep local records of Registration Authority activity including:

- Details of lost or stolen Smartcards.
- Details of all Registration Authority Sponsors and GP RA Agents

14. Registration Authority Reporting

Registration Authority Reporting allows the Registration Authority Team to produce management reports on NCRS users. The Registration Authority Team will produce ad hoc reports on request for any organisation that it provides Registration Authority services to.

In addition to this the Registration Authority Manager will ensure that relevant Sponsors receive regular reports detailing live NCRS User Profiles for their organisation/practice/department/service. The Sponsor will be responsible for ensuring that any anomalies are reported to the Registration Authority Team, so that they can be investigated.

Registration Authority reports containing user details will only be made available to appropriate Registration Authority personnel. Where Registration Authority Reports are saved on computers access will be protected from non-Registration Authority users in keeping with current guidance on person identifiable data. Printed Registration Authority Reports will only be circulated between Registration Authority personnel, and will be handled and stored securely.

15. Cheshire ICT Servicedesk

All Registration Authority requests will be directed through the Cheshire ICT Servicedesk.

Telephone: 0844 800 9982
Email: servicedesk@cheshireict.nhs.uk

16. Reference Documents

The following documents can be found on the documents page of the Integrated Identity Management section of the Connecting for Health website. http://nww.connectingforhealth.nhs.uk/iim/documents

- Registration Authorities Operational Process and Guidance
- National RBAC Database
- Registration Authority Forms (RA01-RA08)

17. Registration Authority Service Agreement for Independent Sector Healthcare Providers and Local Authorities

This Agreement is between **Cheshire ICT Service and …….....** **…….. .** It is intended to guide the inter-organisational governance arrangement between the Parties for the approval, issue, management, and monitoring of Smartcards to NHS Care Record Service users employed by ……., whilst ensuring compliance with all statutory requirements, policies and procedures; as well as Department of Health guidance.

With the introduction of the NHS Care Records Service applications, it is of paramount importance that patients of the NHS are confident that their medical records are being appropriately kept secure and confidential in line with the NHS Care Records Guarantee. To achieve this objective all NHS Care Records Service compliant applications require healthcare professionals/workers who require access, to be registered and issued with a unique identification log-in, known as a Smartcard, and have an appropriate access profile(s).

Cheshire ICT Service Responsibilities

The NHS RA Manager/RA Agent will:

1. Ensure that all NHS RA policies and procedures are adhered to in full.

2. Perform RA Management duties, such as providing routine and appropriate smartcards for ……. staff, where there is a clinical or administrative need to access records of NHS patients, and as described in the published guidelines.

3. Be responsible for providing introductory individual training to Sponsors with regard to their role in PIN management.

4. Be responsible for providing training and guidance material for the use of User Identity Manager

5. Be available to answer queries as required by the Sponsors.

6. Provide and notify 3rd Party Organisation Sponsors of any changes made to RA policies in line with the RA processes and guidelines.

7. Conduct periodic internal audits, if desired, to ensure compliance with NHS RA policies and procedures and reciprocally share the results with Information Governance Staff and 3rd Party Organisation Sponsors/Managers.

8. Provide, as requested, a list of current smartcard users to 3rd Party Organisation Sponsors/Managers.

9. Conduct appropriate card management as per published guidelines.

3rd Party Organisation Sponsor Responsibilities:

1. The ..... Sponsor will identify administrative and clinical users requiring access to records of NHS patients, as described in the published guidelines. The 3rd Party Organisation sponsor will sponsor administration staff only. Clinical staff employed by the 3rd Party Organisation will be sponsored by the CCG Organisational Sponsor.

2. To use User Identity Manager to assign the appropriate level of access to each individual users

3. To use User Identity Manager to create and approve smartcard registration requests.

4. To inform Cheshire ICT Service immediately if a User loses their Smartcard or any other security breach relating to Smartcards occurs.

5. To ensure that user access is removed within a timely fashion when a user leaves the organisation.

6. To ensure all Cheshire ICT Service RA policies and procedures are adhered to in full.

7. To act as PIN manager for smartcards in the event of forgotten passcodes.

8. 3rd Party Organisation Sponsors may not sponsor other sponsors.

9. Ensure compliance with the Data Protection Act 1998, the NHS Confidentiality Code of Practice, Computer Misuse Act 1990.

Responsibilities of Users

1. To keep their smartcard safe and secure at all times
2. Devise and use passcodes known only to themselves for the function of the smartcard
3. Report any security breach they observe of smartcard policy or procedure to the 3rd Party Organisation Sponsor.

CSU Information Governance Manger

Signature	Date

Cheshire ICT Registration Authority Manager

Signature	Date

Third Party Organisation Representative

Signature	Date

Confidentiality and Data Protection Policy

Version	**Version 1**
Ratified By	
Date Ratified	
Author(s)	**Suzanne Crutchley** **Information and Corporate Governance Manager** **CWW Commissioning Support Unit**
Responsible Committee / Officers	
Issue Date	
Review Date	
Intended Audience	**All CCG staff**
Impact Assessed	**Yes**

Further information about this document:

Document name	Confidentiality and Data Protection Policy
Category of Document in The Policy Schedule	Corporate
Author(s) Contact(s) for further information about this document	Suzanne Crutchley Information and Corporate Governance Manager Telephone: 01244 650551 Email: suzanne.crutchley@wcheshirepct.nhs.uk
This document should be read in conjunction with	Information Governance Strategy
Published by	Cheshire, Warrington and Wirral Commissioning Support Unit (CWW CSU)
Copies of this document are available from	Website: http://www.cwwcss.org.uk/extranet or CWW CSU Office, 1829 Building, Countess of Chester Health Park, Liverpool Road, Chester. CH2 1HJ

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

Please note that this Confidentiality and Data Protection Policy is based on the current equivalent for the NHS Business Services Authority, existing PCT Policies, the Information Security Management: NHS Code of Practice, and the Confidentiality: NHS Code of Practice.

Table of Contents

Section **Page**

The following terms are used in this document

Information Governance	Information Governance is a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information.
Information Commissioner's Office	The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Data Protection Principles	All information and data which can identify a person, held in any format (visual/ verbal / paper / computer / microfilm / etc.) is safeguarded by the Data Protection Act 1998, which is underpinned by eight Principles.
NHS Care Record Guarantee	The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this
Caldicott Principles	The Caldicott Principles represent best practice for using and sharing patient identifiable personal information and should be applied whenever a disclosure of personal information is being considered.

1. Introduction

1.1. The Clinical Commissioning Group (CCG) has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information / Information Technology Security. It also has a duty to comply with guidance issued by the Department of Health, and Connecting for Health.

1.2. All legislation relevant to an individual's right to confidentiality and the ways in which that can be achieved and maintained are paramount to the CCG.

1.3. Penalties could be imposed upon the CCG, and / or CCG employees for non-compliance with relevant legislation and NHS guidance.

1.4. This Confidentiality and Data Protection Policy aims to detail how the CCG meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 as that is the key piece of legislation covering security and confidentiality of personal information.

1.5. For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the Data Protection Act 1998, associated legislation and guidance are detailed in Appendix A.

1.6. The NHS and related guidance listed below are the main publications referring to security and or confidentiality of person identifiable data (PID).

- Information Security Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- HSC 1999/012 Caldicott Guardians
- The Caldicott Guardian Manual 2006

2. Policy Statement

2.1. This document defines the Confidentiality and Data Protection Policy for the CCG.

2.2. The Confidentiality and Data Protection Policy applies to all personal information obtained and processed by the CCG and the CCG's employees.

2.3. This document:

- Sets out the organisation's policy for the protection of all information obtained and processed.
- Establishes the responsibilities for Data Protection.
- Provides reference to the Data Protection Act 1998.

3. Principles

3.1. The objective of this policy is to ensure the protection of CCG's information in accordance with the Data Protection Act 1998, that is:

- To ensure notification;
  Annually notify the Information Commissioner about the CCG's use of personal information.
- To ensure professionalism;
  All information is obtained, held and processed in a professional manner in accordance with the eight principles of the Data Protection Act 1998 (which are listed in Appendix A).
- To preserve security;
  All information is obtained, held and disclosed in a secure manner.
- To ensure awareness;
  Proper training and awareness is in place which informs all employees of their roles and responsibilities.
- Data Subject access;
  Prompt and helpful response to any data subject access request.

3.2. The policy and procedure will be reviewed periodically by the CCG Governance Team. Where review is necessary due to legislative change this will happen immediately.

3.3. In accordance with the CCG's Equal Opportunities practice, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

4. Scope of this Policy

4.1. This policy applies to all personal information processed, stored on computer or relevant filing systems (manual records), or Close Circuit Television and any extracts taken either printed, copied, or verbal, together with the CCG staff who use the information in connection with their work.

5. Policy

5.1. The overall Confidentiality and Data Protection Policy for the CCG is described below:

5.2. The CCG needs to obtain and process information about different people for many purposes, for example, but not limited to:

- Pay and Pension
- Work Management
- Staff Training

- Internal Telephone Directory
- Administration of access to information systems
- Smart Card applications
- Email management
- Claims processing
- Staff records and administrative records
- Matters relating to the prevention, detection and investigation of fraud and corruption in the NHS

5.3. Such information may be kept in either computer and/or manual records. In processing such personal data the CCG will comply with the Data Protection principles within the Data Protection Act 1998 (which are listed in Appendix A).

6. Data Protection Responsibilities

Overall Responsibilities

6.1. The CCG permit staff (including contractor staff, temporary staff and work placed students) to use computers and relevant filing systems (manual records) only in connection with their work. The CCG have legal responsibility for the notification process and compliance of the Data Protection Act 1998.

6.2. The CCG, whilst retaining their legal responsibilities have delegated Data Protection compliance to the nominated Data Protection Officer.

6.3. The Data Protection Officer responsibilities have been allocated to the Information Governance Manager within the CCG.

Data Protection Officer's Responsibilities

6.4. The Data Protection Officer responsibilities include:

- Ensuring that an appropriate Data Protection Act 1998 policy for the CCG is produced and kept up to date.
- Ensuring that the appropriate procedures and practices are formulated and adopted by the CCG.
- Representing the CCG on Data Protection matters.
- Providing the appropriate leadership and direction for the Governance Team operating within the CCG.
- Setting the standard of Data Protection Act training for staff across the CCG.
- Ensuring the Data Protection notification is reviewed, maintained and renewed annually for all use of personal information.
- Ensuring compliance with individual's rights, including subject access.
- Acting as a central point of contact on Data Protection within the CCG.
- Implementing an effective framework for the management of Data Protection.

- Monitor compliance with the Data Protection Act 1998, any infringement (i.e. unlawful disclosure of information or access for idle curiosity) are investigated and appropriately dealt with.
- Audit appropriate systems in accordance with risk analysis reviews.
- Assisting with Counter Fraud and Security Management issues

Line Manager's Responsibilities

6.5. All Line Managers across the whole of the CCG are directly responsible for:

- Ensuring that their staff are aware of their Data Protection responsibilities.
- Ensuring that their staff have had suitable Data Protection training.

General Responsibilities

6.6. All CCG employees (including contractor staff, temporary staff and work placed students) are subject to Data Protection compliance and this policy. They are accountable via personal liability.

6.7. All CCG employees (including contractor staff, temporary staff and work placed students) have a responsibility to inform the Data Protection Officer of any new use of Personal Data as soon as possible after it has been identified.

7. Staff Code of Conduct

7.1. To ensure staff members are effectively informed of what is required of them, the CCG has a Staff Code of Conduct (code) that identifies legal requirements and best practice.

7.2. The code applies to all the different staff groups, e.g. for staff working with particularly sensitive information or those who have little access to confidential information.

7.3. The code is set out as follows:

a. The legal framework and the circumstances under which confidential information can be disclosed

National guidance includes NHS Codes of Practice on Confidentiality, Records Management and Information Security Management; the Caldicott Principles; and the NHS Care Record Guarantee for England. Care professionals must also comply with the codes of practice of their respective professions. These national guidelines also provide a basis for local codes which can focus on particular work areas or staff groups. The Caldicott Principles and the relevant extracts from the Care Record Guarantee are set out below.

b. The NHS and Social Care Record Guarantees for England

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. The Guarantee was first published in 2005 and is reviewed annually by the National Information Governance Board. The Social Care Record Guarantee - published in 2009 - explains to service users how the information they provide to social care staff is used and what control they can have over this. It complements the NHS Care Record Guarantee for England.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

c. The Caldicott Principles

The Caldicott Principles were devised by the Caldicott Committee, which reported in 1997 following a review of patient-identifiable information. They represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered.

- Principle 1: Justify the purpose for using the information
- Principle 2: Only use it when absolutely necessary
- Principle 3: Use the minimum that is required
- Principle 4: Access should be on a strict need to know basis
- Principle 5: Everyone must understand their responsibilities
- Principle 6: Understand and comply with the law

d. The systems and processes for protecting personal information

These include all safe haven procedures, e.g. for answering telephone queries or receiving confidential faxes, any information sharing protocols agreed with external organisations, encryption requirements for mobile devices and secure transfers of personal information.

e. Who to approach within the CCG for assistance and advice on disclosure issues

There are a range of individuals who can assist with difficult issues – the Information Governance lead, Caldicott Guardian, Senior Information Risk Owner, and Data Protection lead can be approached.

f. Possible sanctions for breach of confidentiality or data loss

The CCG will ensure that all staff members are aware of the possible disciplinary sanctions for failure to comply with their responsibilities, e.g. deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal information electronically without encrypting it, etc. Sanctions can include disciplinary action, ending a contract, dismissal, or bringing criminal charges. Since April 2010, the Information Commissioner's Office (ICO) may order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998.

g. Staff Awareness

The CCG will ensure that staff are effectively informed about the code through awareness sessions, team meetings, briefing notes or a combination of these. The code must be accessible so it needs to be readily available – it will be published on the Internet. Understanding what is required should be supported through staff training, e.g. through the on-line NHS Information Governance training modules, which all staff can access through the National Learning Management System (NLMS).

8. Validity of this Policy

8.1. This policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

8.2. This policy will be reviewed annually by the CCG Governance Team members. Associated Data Protection standards and procedures will be subject to an on-going development and review programme.

Appendix A

Associated Legislation and Guidance

Data Protection Act 1998 - Data Protection Principles
All information and data which can identify a person, held in any format (visual/ verbal / paper / computer / microfilm / etc.) is safeguarded by the Act, which is underpinned by eight principles.

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Human Rights Act 2000
This Act binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public CCG with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000
This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000
This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998
This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local CCG boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local CCG boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990
This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records 1990
This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988
This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

The Telecommunications (Lawful Business Practice) (Interception of

Communications) Regulations 2000
This Act defines the scope for legitimate monitoring of communications within an organisation

Obscene Publications Act 1959
This Act makes it an offence to publish or distribute pornography.

Communications Act 2003
This Act makes it an offence to transmit grossly obscene or offensive messages or untrue messages designed to cause annoyance, inconvenience or needless anxiety.

Protection of Children Act 1978
This Act makes it an offence to possess child pornography. Possession includes viewing such material as well as downloading or storing it.

Copyright, Design and Patents Act 1988
This Act is applicable to all types of creations, including text, graphics and sounds by an author or an artist. Any unloading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of his / her rights The application of the Copyright Act to electronic copying is even stricter than its application to photocopying, since the fair dealing arrangements which usually apply to libraries (i.e. one article per journal for the purposes of research or private study) do not exist for computerised materials.

Some types of infringement give rise to criminal offences, the penalties for which may amount to up to two years' imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by injunction

Protection from Harassment Act 1997
This Act was passed following concern that stalking was not suitably dealt with under existing legislation, however it does not refer solely to stalking and covers harassment in a wider sense. The Act says that it is unlawful to cause harassment, alarm or distress by a course of conduct and states that:

> *A person must not pursue a course of conduct*
> *(a) which amounts to harassment of another, and*
> *(b) which he knows or ought to know amounts to harassment of the other.*

Sex Discrimination Act 1975
This Act states that it is unlawful to discriminate against a person on the grounds of their sex or marital status

Race Relations Act 1976
This Act states that it is unlawful to discriminate against a person on the grounds of race, colour, nationality, citizenship or ethnic origins.

Information Security Management: NHS Code of Practice
This is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to,

or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice.

Confidentiality: NHS Code of Practice
Gives NHS bodies guidance concerning the required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. It replaces previous guidance, HSG (96)18/LASSL (96) 5 – The Protection and Use of Patient Information and is a key component of the information governance arrangements for the NHS.

Records Management: NHS Code of Practice
Acts as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

HSC 1999/012 Caldicott Guardians, and
The Caldicott Guardian Manual 2006
Provide guidelines relating to sharing of patient identifiable information and promote the appointment of a senior health professional to oversee the implementation of the guidance.

Corporate Records and Retention Policy

Policy for the local management of the Records Management: NHS Code of Practice

Version	**Version 1**
Ratified By	
Date Ratified	
Author(s)	**Suzanne Crutchley** **Information and Corporate Governance Manager** **CWW Commissioning Support Unit**
Responsible Committee / Officers	
Issue Date	
Review Date	
Intended Audience	**All CCG staff**
Impact Assessed	**Yes**

Further information about this document:

Document name	Corporate Records and Retention Policy *Policy for the local management of the Records Management: NHS Code of Practice*
Category of Document in The Policy Schedule	Corporate
Author(s) Contact(s) for further information about this document	Suzanne Crutchley Information and Corporate Governance Manager Telephone: 01244 650551 Email: suzanne.crutchley@wcheshirepct.nhs.uk
This document should be read in conjunction with	• Information Governance Strategy • Information Governance Policy • Freedom of Information Policy
Published by	Cheshire, Warrington and Wirral Commissioning Support Unit (CWW CSU)
Copies of this document are available from	Website: http://www.cwwcss.org.uk/extranet or CWW CSU Office, 1829 Building, Countess of Chester Health Park, Liverpool Road, Chester. CH2 1HJ

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

Please note that this Policy is based on the current equivalent for the NHS Business Services Authority, existing PCT Policies and the Records Management: NHS Code of Practice.

Contents

Section **Page**

The following terms are used in this document

Information Governance	Information Governance is a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information.

Glossary of Records Management Terms

Full descriptions of all the terms used in the Records Management: NHS Code of Practice are listed in full in the Code, available at: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

1. INTRODUCTION AND PURPOSE

1.1 Introduction

NHS organisations have a statutory duty to make arrangements for the safekeeping and eventual disposal of their records.

The primary function of the Policy is to improve the management of all types of NHS records, with regard to their preservation, retention and destruction.

The suggested retention periods should be taken by NHS organisations to be a guide based on best practice, and therefore followed for all corporate (non-clinical) records.

Ensuring local application of this Policy and its supporting guidelines and procedures, is the responsibility of all staff.

1.2 Executive Summary

The Corporate Records and Retention Policy for the Clinical Commissioning Group (CCG) sets out the requirements of all staff when managing the retention of records. The Policy is supported by substantial guidelines and procedures, which give further details of how to comply with the actual Policy.

Staff should treat this Policy as guidance based on best practice for managing corporate records. In general terms, this Policy covers all records (documents), which the CCG has produced.

The records management function is recognised as a specific corporate responsibility within the CCG. It provides a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. All confidential papers will be disposed of by shredding.

Clearly defined responsibilities and objectives are set out below, and the CCG is committed to ensure adequate resources to achieve them.

This Policy should be read in conjunction with the following CCG Policies:

- Information Governance Strategy
- Information Governance Policy
- Freedom of Information Policy

Archiving of corporate paper documents will be carried out in line with the CCG arrangements in place, which will be reviewed over time as the CCG develops.

1.3 Foreword

This Policy has been produced in light of the requirements of the *Records Management: NHS Code of Practice,* and should be read in conjunction with the full Code. To download a copy of the Code of Practice please follows this link http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

The *Records Management: NHS Code of Practice* has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. The Code of Practice (referred to as the Code) is a guide to the standards of practice required in the management of NHS records, based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type.

This Policy supports, amongst others, the Data Protection Act 1998 and the Freedom of Information Act 2000.

The life of this Policy will be subject to controlled amendments ensuring it remains appropriate as the business, technology and legislation change. This Policy and its supporting guidelines and procedures will be regularly reviewed and compliance with them monitored through Risk Management and Information Governance Assurance procedures. The policy will be reviewed at regular intervals (at least once every two years) and, if appropriate, it will be amended to maintain its currency and relevance.

1.4 Types of record covered by the Code of Practice

The guidelines contained in the Code of Practice apply to NHS records of all types, regardless of the media on which they are held. These may consist of:

- Administrative records (including, for example, personnel, estates, financial and accounting records; notes associated with complaint-handling);
- Photographs, slides, and other images;
- Microform (i.e. microfiche/microfilm);
- Audio and video tapes, cassettes, CD-ROM etc;
- E-mails;
- Computerised records;
- Paper records;

- Scanned records;
- Text messages (both outgoing from the NHS and incoming responses)

1.5 Background and general context

The *Records Management: NHS Code of Practice* replaces previous guidance as listed below:

- HSC 1999/053 – *For the Record*.
- HSC 1998/217 – *Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients* (Replacement for FHSL (94)(30))
- HSC 1998/153 – *Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice.*

Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed. An effective records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required. Information may be needed:

- to support patient care and continuity of care;
- to support day-to-day business which underpins the delivery of care;
- to support evidence-based clinical practice;
- to support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
- to meet legal requirements, including requests under subject access provisions of the Data Protection Act or the Freedom of Information Act;
- to assist clinical and other types of audits;
- to support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research; or
- to support patient choice and control over treatment and services designed around patients.

The Code of Practice identifies the specific actions, managerial responsibilities, and minimum retention periods for the effective management of all types of NHS records (i.e. both corporate and health records) from creation, as well as day-to-day use of records, and storage, maintenance and ultimate disposal procedures.

1.6 Policy and Strategy

The CCG policy on how it manages all of its records, including electronic records is endorsed by the Governing Body and will be made readily available to all staff at all levels of the CCG, both on induction and through regular update training.

The policy sets out the CCG's commitment to create, keep and manage records and document its principal activities in this respect.

The policy also:

- outlines the role of records management within the CCG, and its relationship to the CCG's overall strategy;

- defines roles and responsibilities within the CCG, including the responsibility of individuals to document their actions and decisions in the CCG's records, and to dispose of records appropriately when they are no longer required;

- provides a framework for supporting standards, procedures and guidelines; and

- indicates the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained.

2. KEY PERFORMANCE INDICATORS

2.1 The following key performance indicators have been identified to measure the effectiveness of this document:

a) staff will know where to access the document;

b) staff will know how to archive documents;

c) policy to be reviewed by the review date.

3. SCOPE OF THE POLICY

3.1 This Policy applies to all employees of the CCG, both permanent and temporary.

3.2 It also applies to anyone contracted to the CCG, who, in the course of their work is required to create and/or access corporate records normally restricted to directly employed staff.

4. OBJECTIVES OF THE POLICY

4.1 NHS Records Management

The aims of the NHS Code of Practice are:

- to establish an Information Governance framework for NHS records management in relation to the creation, use, storage, management and disposal of all types of records;
- to clarify the legal obligations that apply to NHS records;
- to explain the actions required by the CCG senior managers to fulfil these obligations;
- to explain the requirement to select records for permanent preservation;
- to set out recommended minimum periods for retention of all types of NHS records, regardless of the media on which they are held; and
- to indicate where further information on records management may be found.

4.2 Corporate Records Retention Policy

The objectives of this Policy are to:

- Make all staff aware of their responsibilities for the retention of corporate records.
- Introduce a retention schedule for the CCG's corporate records.
- Create a controlled environment and formal methods of destruction of corporate records.

5. ROLES AND RESPONSIBILITIES

5.1 A ***designated member of staff*** of appropriate seniority (i.e. Governing Body level or reporting directly to a Governing Body member) will have ***lead responsibility for Records Management*** within the CCG. This lead role will be formally acknowledged and made widely known throughout the CCG.

5.2 **The *Chief Operating Officer*** is personally accountable for records management within the CCG and has a duty to make arrangements for the safekeeping of those records. Each CCG Department must have a comprehensive records management programme which includes cost-effective management of non-current as well as active records, and which takes account of 'Risk Management' principles.

5.3 ***Senior Managers*** must give their full backing to all the guidelines and procedures as set out and agreed. Senior Managers must also take responsibility to ensure that:

- All new staff will receive training/guidance in the retention of records, within one month of joining the CCG.
    - All existing staff are made aware of their responsibilities.
- There is adequate disposal arrangements for confidential waste, which all staff abide by.
- There is adequate storage facilities for back-up media and other storage devices, which contain person identifiable information and sensitive/confidential corporate/staff information.

5.4 ***All line managers and supervisors*** must ensure that their staff are adequately trained and apply the appropriate guidelines.

5.5 ***The Caldicott Guardian*** is responsible within the CCG for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential patient information are in place.

5.6 ***The Senior Information Risk Owner*** (SIRO) is responsible within the CCG for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential corporate information and person identifiable information (non-patient) are in place.

5.7 ***Each individual*** has a key role to play in effective record keeping. Everyone working for or with the NHS who records, handles, stores, or otherwise comes across information has a personal responsibility to apply the appropriate guidelines for the retention and eventual destruction of information.

5.8 Under the Public Records Act all NHS employees are responsible for any records that they create or use in the course of their duties. Thus any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations. A description of these obligations can be found in Annex C of the Code.

5.9 It is essential that the manager(s) responsible for the records management function will work in close association with the manager(s) responsible for freedom of information, data protection and other information governance work areas.

5.10 All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities in respect of record keeping and records management, and that they are competent to carry out their designated duties. This should include training for staff in the use of electronic records systems. It should be done through both generic and specific training programmes,

complemented by CCG policies and procedures and guidance documentation. For example, the designated Records Manager who has overall responsibility for managing the 'records libraries' and other storage areas where records are kept, must have an up-to-date knowledge of, or access to expert advice on, the laws and guidelines concerning confidentiality, data protection (including subject access requests), and freedom of information.

5.11 Corporate records are core resources for the CCG. They must be properly formatted, produced consistently, safeguarded and used efficiently, and all staff (managerial, administrative, professional and medical) must follow this Policy and its supporting guidelines and procedures.

5.12 All NHS records are public records under the terms of the Public Records Act 1958 sections 3 (1)–(2). The Secretary of State for Health and all NHS organisations have a duty under the Public Records Act to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

5.13 Directors and Senior Managers of all NHS organisations are personally accountable for records management within their organisation. NHS organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor organisations and/or obsolete services.

5.14 In addition, NHS organisations need robust records management procedures to meet the requirements set out under the Data Protection Act 1998 and the Freedom of Information Act 2000.

6. MONITORING RECORDS MANAGEMENT PERFORMANCE

6.1 A number of bodies monitor NHS performance in respect of records management. The Audit Commission regularly conducts studies into records management and related information quality issues. The Department of Health collects performance details as part of the annual Information Governance Toolkit assessment and these will inform the work of both the Healthcare Commission and the Audit Commission. The NHS Litigation Authority also undertakes a risk assessment survey as an integral part of the Clinical Negligence Scheme for Trusts (CNST).

6.2 Other bodies likely to comment on records management performance include the Information Commissioner when investigating alleged breaches of Data Protection or Freedom of Information legislation or in promoting the Lord Chancellor's Code of Practice on Records Management under section 46 of the Freedom of Information Act.

7. LEGAL AND PROFESSIONAL OBLIGATIONS

7.1 All individuals who work for an NHS organisation are responsible for any records which they create or use in the performance of their duties. Furthermore, any record that an individual creates is a public record.

7.2 The key statutory requirement for compliance with records management principles is the Data Protection Act 1998, where personal information is held. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records. Therefore the same principles apply to records of employees and contract workers held by employers, for example in finance, personnel and occupational health departments.

8. NHS CONNECTING FOR HEALTH

8.1 The impact of the Government's health reform agenda will fundamentally affect the way the NHS approaches the management of all electronic records. The NHS Care Records Service (NHS CRS) and other initiatives are central to these reforms and will transform the way both health and social care information is managed.

9. RECORD CREATION

9.1 Records of operational activities should be complete and accurate in order to allow employees and their successors to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of the CCG by anyone so authorised, to protect the legal and other rights of the CCG, its staff and any other people affected by its actions, and provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

9.2 Records created by the CCG should be in Corporate House Style and arranged in a record-keeping system that will enable the CCG to obtain the maximum benefit from the quick and easy retrieval of information. The main system used is the Extranet. If not the Extranet, then a system to which more than one person has routine access and the system(s) is known by more than one person.

10. INFORMATION QUALITY ASSURANCE

10.1 It is important that all NHS organisations train staff appropriately and provide regular update training. In the context of records management and information quality, organisations need to ensure that their staff are fully trained in record creation, use and maintenance, including having an understanding of:

- what they are recording and how it should be recorded;

- why they are recording it;

- how to validate information against other records – to ensure that staff are recording the correct data;

- how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;

- the use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and

- how to update information and add in information from other sources.

10.2 Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions (for example finance, IT, HR). A Department information survey or record audit is essential to meeting this requirement. This survey will also help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

10.3 Paper and electronic record keeping systems should conform to the Corporate House Style and should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

10.4 The record keeping system should either adhere to the Corporate House Style or should include a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information when it is needed and to maintain security and confidentiality.

11. RECORD KEEPING

11.1 The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

11.2 Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

11.3 For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.

11.4 Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

11.5 When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. There should be archiving procedures in place for both paper and electronic records.

11.6 A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the CCG. Key expertise in relation to environmental hazards, assessment of risk, business continuity and other considerations is likely to rest with information security staff and their advice should be sought on these matters.

12. RECORD MAINTENANCE

12.1 For reasons of business efficiency or in order to address problems with storage space, NHS organisations may consider the option of scanning into electronic format records which exist in paper format. Where this is proposed, the factors to be taken into account should be taken from the Code.

13. DISCLOSURE AND TRANSFER OF RECORDS

13.1 There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. The key statutory requirements can be found in Annex C of the Code. Designated staff within the CCG have special expertise in, or can advise on, particular types of disclosure e.g. the Caldicott Guardian and the Senior Information Risk Owner.

13.2 The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity and confidentiality of the material contained within the records and the media on which they are held. Information Security staff can advise on appropriate safeguards.

14. RETENTION AND DISPOSAL ARRANGEMENTS

14.1 Detailed guidance on retention periods for a full range of NHS personal health and different types of business and corporate records is provided in Annex D of the Code.

14.2 It is particularly important under freedom of information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed – is undertaken in accordance with clearly established policies which have been formally adopted by the CCG and which are enforced by properly trained and authorised staff.

14.3 Archiving of corporate paper documents will be carried out in line with the CCG arrangements in place.

15. APPRAISAL OF RECORDS

15.1 Appraisal refers to the process of determining whether records are worthy of permanent archival preservation. This should be undertaken in consultation with the CCG Managers who have 'records management' responsibilities.

15.2 The retention schedules in Annex D of the Code outline the recommended minimum retention periods for all types of NHS records. The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

16. RECORD CLOSURE

16.1 Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes.

16.2 An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders.

16.3 Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

17. RECORD DISPOSAL

17.1 The CCG retention/disposal schedule is taken from the retention schedules contained in the Code. The CCG schedule covers all records held by the CCG, including electronic records.

17.2 In the event of any records selected for archival preservation and no longer in regular use by the CCG, these will be transferred as soon as possible to an archival institution (for example a Place of Deposit – see Annex E of the Code) that has adequate storage and public access facilities.

17.3 It is the responsibility of the CCG to ensure that the methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Most NHS records are confidential records. All confidential papers will be disposed of by shredding.

17.4 A record of the destruction of records, showing their reference, description and date of destruction will be maintained and preserved by the nominated Records Manager, so that the CCG is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules will constitute the basis of such a record.

17.5 If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act 2000 have been exhausted or the legal process completed.

18. INFORMATION LIFECYCLE MANAGEMENT

18.1 Information Lifecycle Management is included within this Corporate Records and Retention Policy.

18.2 All NHS records produced are subject to a range of legislation, including the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

18.3 Information Lifecycle Management guides staff on the appropriate manner for the creation, storage, maintenance, use, archiving and disposal of it corporate records.

18.4 It is important that employees recognise information security issues arising from the storage of person identifiable data (PID) and that they continue to use information in accordance with the Data Protection and Freedom of Information Acts, and the NHS Records Management Code of Practice.

18.5 For broader guidance on corporate records management, this statement should be read in conjunction with the following policies:

- Freedom of Information Policy (which includes the Environmental Information Regulations 2004)
- Information Governance Strategy

18.6 The Caldicott Guardian continues to be responsible for protecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring that patient identifiable information is shared in a secure and responsible manner.

18.7 The Senior Information Risk Owner (SIRO) continues to be responsible for ensuring that identified *information threats* are followed up and risks managed.

Annex: Records Retention Schedule

The following is taken from the Records Management: NHS Code of Practice *Annex D2: Business and Corporate (Non-Health) Records Retention Schedule* available at:

http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_093028.pdf

This retention schedule details a minimum retention period for each type of non-health record. Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. The National Archives (see Note below) should be consulted where a longer period than 30 years is required, or for any pre-1948 records. Organisations should also remember that records containing personal information are subject to the Data Protection Act 1998.

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- administrative records (including personnel, estates, financial and accounting
- records, and notes associated with complaint handling)
- photographs, slides and other images (non-clinical)
- microform (i.e. microfiche/microfilm)
- audio and video tapes, cassettes, CD-ROMs, etc
- e-mails
- computerised records; and
- scanned documents

The schedule is split into the following types of records:

- Administrative (corporate and organisation)
- Biomedical Engineering
- Estates/engineering
- Financial
- IM & T
- Other
- Personnel/human resources

- Purchasing/supplies

Notes

An organisation with an existing relationship with an approved Place of Deposit should consult the Place of Deposit in the first instance. Where there is no preexisting relationship with a Place of Deposit, organisations should consult The National Archives.

N.B. only the first page is shown here for reference for the Committee
(the complete Table is 42 pages long)

The whole *Annex D2: Business and Corporate (Non-Health) Records Retention Schedule* is available at:
http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_093028.pdf

TYPE/SUBTYPE OF RECORD	MINIMUM RETENTION PERIOD	DERIVATION	FINAL ACTION	CODE
ADMINISTRATIVE (CORPORATE AND ORGANISATION)				
Accident forms (see also Litigation dossiers)	10 years		Destroy under confidential conditions	S
Accident register (Reporting of Injuries, Diseases and Dangerous Occurrences register) – see also Incident forms	10 years	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (reg. 7); Social Security (Claims and Payments) Regulations (reg. 25)	Destroy under confidential conditions	C

Information Governance Induction and Annual Refresher Training Procedure

Contents

1 BACKGROUND

1.1 Fundamental to the success of delivering the Information Governance Strategy is developing an Information Governance culture within the Primary Care Trust. Awareness and training needs to be provided to all staff, who utilise information in their day-to-day work to promote this culture.

1.2 In order to achieve this a mandatory annual training plan has been agreed across the organisation. This is in line with a Department of Health requirement.

1.3 All staff, clinical and non-clinical, agency and contractor, are required to complete the mandatory course: *Introduction to Information Governance.* Staff have to complete the on line National Learning Management System (NLMS) Information Governance training by 30th June 2011, and then a refresher once a year thereafter.

2 KEY PERFORMANCE INDICATORS

2.1 The following key performance indicators have been identified to measure the effectiveness of this document:

d) Staff will know where to access the training

e) Staff will complete the training each year

3 SCOPE

3.1 Information Governance is a framework concerning the way that information about patients, employees and contractors is handled. It is particularly concerned with personal and sensitive information, but it also incorporates corporate confidential information about the NHS organisation – i.e. your Primary Care Trust.

3.2 Information Governance applies to all employees of the Primary Care Trust, both permanent and temporary. It also applies to anyone contracted to the Primary Care Trust, who, in the course of their work is required to access information and systems normally restricted to directly-employed staff.

4 OBJECTIVES

4.1 The objectives of this Procedure are to set out what staff are required to do in respect of Information Governance training:

- **All staff**, clinical and non-clinical, are required to complete the **mandatory** course: ***Introduction to Information Governance***
- Staff have to complete the on line NLMS Information Governance training by **30th June 2011**, and then a refresher once a year thereafter.
- Staff have to complete a **refresher** once a year thereafter.

5 QUESTIONS & ANSWERS

5.1 Why do I have to complete an e-learning module?

It is a Department of Health requirement that all staff complete the "Introduction to Information Governance" e-learning module. The module has been designed to be user friendly and promote consistency and good practice across the NHS.

5.2. What does the module cover?

The "Introduction to Information Governance" module covers Data Protection, confidentiality, Freedom of Information, good record keeping and information security.

5.3 When do I have to complete it by and how long will it take?

For all staff, the module must be completed by **30th June 2011**. It should take around one hour and there is a short assessment at the end. The module will automatically bookmark if you do not get a chance to finish it in one go.

6 NLMS OVERVIEW

6.1 The National Learning Management System (NLMS) is the nationally developed e-learning solution providing a web based e-learning tool for the NHS with an integrated learning management system connected to the Electronic Staff Record.

6.2 E-learning is now being increasingly used in the NHS, as an alternative to classroom based training.

7 HOW TO ACCESS THE NATIONAL LEARNING MANAGEMENT SYSTEM

7.1 All CCG computers have been approved for their compatibility with the system. Every member of staff based should now have been sent a personal email containing their unique username and password for the National Learning Management System, along with guidance on how to access the system.

The username and passwords were primarily sent to NHS net accounts if available, otherwise from PCT accounts.

Getting Started on NLMS

All staff should now have a link on their desktop taking them to the National Learning Management System login page, which is: https://esr.mhapp.nhs.uk/OA_HTML/AppsLogin

If your link does not work, please contact Cheshire ICT Service on 0844 800982 to report the problem.

The following link takes you directly to the support page for the National Learning Management System: http://www.esrsupport.co.uk/nlms/

NLMS Instructions to enrol on to a course

The following web link, takes you through to a helpful tutorial to enrol on to a course: http://www.esrsupport.co.uk/nlms/OLM_Enrol_Play/Enrol_Play.htm

The course that you are required to complete is:

000 Introduction to Information Governance
(course code: IG_02)

8 OTHER INFORMATION GOVERNANCE TRAINING MODULES

8.1 There are other Information Governance learning tools (training modules) available through the on line Information Governance Training Tool, which can be found at: http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm?action=logout

8.2. The learning tools cover:

- Confidentiality & Caldicott
- Information Governance and IG Management
- Information Security
- Records Management

8.3. Further information about the on line Information Governance Training Tool can be found at Appendix C.

8.4. The learning tools are set out in a table available at. https://www.igte-learning.connectingforhealth.nhs.uk/igte/training.cfm

8.5. There is also 'Information Governance: The Refresher Module' available through the Information Governance Training Tool, which all staff should complete on a rolling annual basis.

9 STAFF INDUCTION INFORMATION GOVERNANCE CHECKLIST

9.1 Please see the following checklist which should be completed ***in the first week of employment:***

APPENDIX A: Staff Induction Information Governance Checklist

10 STAFF TRAINING NEEDS ANALYSIS FOR INFORMATION GOVERNANCE

10.1 On occasions (e.g. following a security incident or near miss) staff may need to have localised refresher training on some aspects of Data Security and Confidentiality. Please see the following Training Needs Analysis to assess such need:

APPENDIX B: Staff Training Needs Analysis for Information Governance

11 FURTHER HELP

Further Help with NLMS

All queries about usernames or passwords (including new staff requiring access) should be directed to the Cheshire, Warrington, Wirral HR Service workforce information team at:
wc-pct.workforceinformation@nhs.net

Existing staff who have not yet been issued their usernames and passwords should contact the Cheshire, Warrington, Wirral HR Service:

Problems with NLMS should be directed to Dennis O'Higgins, L&D Systems Manager, based at Congleton, directly on 01606 544947 or 01606 544948.

Further Help with Information Governance

Suzanne Crutchley LL.M
Information Governance Manager
Tel: 01244 650551
Email: suzanne.crutchley@wcheshirepct.nhs.uk

APPENDIX A

Staff Induction Information Governance Checklist

Employee Name _____ Job Title _____

Directorate _____ Department _____

Managers Name _____ Job Title _____

Date Employee Commenced Employment in current role _____

This form should be completed in the first week of employment

The following topics have been covered during my induction:

- Physical Security of Manual Records □
- Physical Security of Computer Records □
- Access to Person Identifiable Data □
- Confidentiality and the use of Person Identifiable Information, including Information Sharing Protocols when needed □
- Corporate Archive Store □
- Media Handling (Storage/transfer/disposal) □
- Telephone Enquiries □
- Safe Haven Procedures □
- Legal Requirements, including 'subject access' and 'freedom of information' requests □
- Caldicott Guardian Guidelines □
- Role of the Senior Information Risk Owner □
- Building Security □

Signature of Employee _____Date_____

Signature of Manager _____Date_____

APPENDIX B

Staff Training Needs Analysis for Information Governance

On occasions (e.g. following a security incident or near miss) staff may need to have localised refresher training on some aspects of Data Security and Confidentiality. This document is designed to act as a guide when such training is being assessed.

Employee Name _____

Job Title _____

Does the member of staff need training on the following topics?

	Yes	No	Unsure
Physical Security of Manual Records			
Physical Security of Computer Records			
Access to person identifiable data (PID)			
Confidentiality and the use of person identifiable data			
Privacy Impact Assessments			
Information Sharing Protocols			
Media Handling (Storage/Transfer/Disposal)			
Corporate Archive Store			
Telephone Enquiries			
Safe Haven Procedures			
Legal Requirements: 'subject access requests'			

Legal Requirements: freedom of information' requests			
Caldicott Guardian Guidelines			
Role of the Senior Information Risk Owner			
Security of the Building			

Are there any other areas of Information Governance that the member of staff needs further training on?

yes / no

If yes, outline them below:

……

……

……

Signature of Employee _____

Date _____

Action / Training plan:

……

……

……

Target Date _____ Completion Date _____

Name of Manager _____

Job Title _____

Signature of Manager _____

Date _____

APPENDIX C

What is the IG Training Tool?

The **IG Training Tool** is an online training tool focused on all aspects of learning about Information Governance (IG). The aim of the tool is to develop and improve staff knowledge and skills in the IG work area, to support the provision of high-quality health & social care.

This tool provides you with introductory, foundation and practitioner level training materials, to support you in learning all you need to know about IG. It allows you to learn about essential IG topics, test your knowledge once you have completed the modules and read more about the topics if you are interested to know more. It also stores your training progress as you go through the e-learning training.

The tool is only available online which allows the information to be kept up-to-date. This makes sure you're kept informed of the latest IG best practice, and new or amended legislation.

What's in the IG Training Tool?

The tool consists of a range of materials to accommodate your training needs and preferences. These are divided into three main sections:

Learning tools tab – in this section you will find a range of e-learning modules; each module contains three sections:

> **Learn all about it** - containing e-learning training.
> **Check what you know** - containing an assessment. If you score 80% or more you will pass and gain a certificate.
> **Read all about it** - displays links to useful information for further reading on topic areas covered within the e-learning.

Trainer materials tab – this section contains a selection of PowerPoint presentations accompanied by scripted notes and audio clips for face-to-face training.

http://www.igte-learning.connectingforhealth.nhs.uk/igte/training.cfm

- Audio role plays (49 resources)
- Confidentiality & Caldicott (10 resources)
- Information Governance and IG Management (19 resources)
- Information Security (15 resources)

Resource library tab – in here you can search for any training materials or useful links which appear within the whole training tool site at a click of a button. There is a search engine which allows you to word search by title or you can click on the headings of each column and sort alphabetically.

The e-learning training and assessments must be taken online, but the reference materials can be read online, or downloaded, printed and read at your leisure.

Other sections:

News – this will inform you of any new modules released or updates made to the IG training tool. It will also relay general information.

Your profile – allows you to update your registration information and change your password regularly yourself.

Help – this is where you can pose questions to our subject matter experts if you are still unsure about certain topics covered within the training materials, if you are having problems using the tool in any way or if you need further guidance in terms of IG. You can also contact the team via email exeter.helpdesk@nhs.net or telephone 01392 251289.

Access to the IG Training Tool is free and the content is directed at NHS Trusts, Social Care organisations and General Practices. Materials may also be suitable for Third Party organisations involved with the implementation of the NPfIT or engaged in contracts with NHS organisations.

Information Governance

SPOT CHECKS FOR SAFE HAVEN PROCEDURES

Each organisation should establish safe-haven administrative arrangements to safeguard confidential corporate and person-identifiable information.

Date of Report:	January 2013
Organisation:	Wirral CCG
Location:	Old Market House, Birkenhead
Staff spoken to: (during November 2012)	These included: Administrators Executive Team staff Commissioning Managers
General Observations:	Open plan office areas with limited access by the public. However, it is possible to get to each floor of the building, without a *door swipe card*, as there are push buttons within easy reach at the main entrance of the building, and *disabled user push buttons* which open most doors on most floors to get in to office areas. Good knowledge and observance of Information Governance requirements in general. Very few paper documents held as vast majority of information is held and processed electronically. IPads are used for key meeting papers (use *Good Reader* software), rather than printing off paper copies.
Recommendations:	The CCG should speak to the 'landlord' for the building to see if areas of the building could be further protected from **general access**. The CCG should consider replacing their **fax machine**, which is needed as part of Business Continuity Planning, with a newer model which would allow for storing ***frequently used numbers*** and stopping documents being printed 'out of hours' (activated the next morning by a ***PIN code***). The CCG should provide a template ***'front cover sheet'*** for use when faxing documents. The CCG should remind staff who have yet to complete their **annual Information Governance training**.

	The CSU are looking in to securing the most cost-effective **offsite storage** for the CCGs across Cheshire, Warrington, and Wirral. The CCG should wait for this to be finalised and then consider the minimum key paper documents for offsite storage.

Who is your Caldicott Guardian?

Yes ✓ All staff were unaware of who the Caldicott Guardian is.

Who is your Senior Information Risk Owner?

Yes ✓ All staff were unaware of who the SIRO is.

Facsimile Machines

- *Facsimile machines are sited in areas where the general public does not have physical access.*

  One fax machine within the CCG offices is used if needed. The CCG should consider buying a new fax machine, which is needed as part of Business Continuity Planning.

- *Secure arrangements are made for the confidential handling of transmitted data / information which may be received outside of normal working hours.*

  No X Limited CCG control in place.

- *Frequently used numbers have been identified and programmed into the fax machine "memory dial" facility to reduce risk of misdialling.*

  No X No CCG control in place.

- *All faxes sent include instructions on the fax cover sheet for the process of handling misdirected facsimile information.*

  Yes ✓ But, the CCG should provide a template 'front cover sheet' for use when faxing documents.

Computers

- *Users 'lock' or 'log off' from their computer when away from their desk*

  Yes ✓ Windows + L, or Control + Alt + Delete is used to lock the computer.

- *Computer screens are positioned so they are not visible to patients/public*

Yes ✓ Office not readily accessible by patients or public.

- *Screen Savers are set to activate, at Network level, when there is no activity for a short pre-determined period of time.*

  Yes ✓

- *Screen savers are password protected for reactivation.*

  Yes ✓

Other Electronic Media

- ***Dictation machines** and tapes are always kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed.*

  Not applicable as none held ✓

- ***Portable Media** held is logged through WHIS and encrypted.*

  IPads, laptops, and memory sticks have all been issued through WHIS and are encrypted ✓

- *There is an area available for staff to use the **telephone** away from the public. One telephone in the department should be designated the Safe Haven telephone.*

  CCG staff have access to various meeting rooms and smaller offices, where confidential telephones calls can be made ✓

- ***Ansaphones** are located in a secure area.*

  Not applicable as none held ✓

- ***Photocopying machines** are sited in areas where the general public does not have physical access.*

  Yes ✓

- ***Photographic / Video media** is kept in a secure area.*

  Not applicable as none held ✓

Manual Records and Books

- *Message Books, Visitor Books, Appointment Books and other written records, which contain Person Identifiable Information (PID) or other confidential or sensitive information, are sited away from the general public and are stored in a locked area when not in use.*

  Yes ✓

Post

- *Post in and post out trays are sited away from the general public and stored in an area with controlled access.*

  Yes ✓

Clear Desk Procedures

- *At the end of each working session all 'sensitive' information is removed from the work place and stored in a locked area (this includes all patient identifiable information, as well as business critical information such as salaries and contracts).*

  Lockable drawers and cupboards used to store confidential documents/information ✓

- *Before a patient enters a consulting room all evidence of the previous patient is removed from view (computer screens, medical records, test papers or samples, etc).*

  Not applicable ✓

- *All consulting rooms and office areas are locked when they are not in use.*

  No X Within the open plan office the smaller office doors are not locked, but confidential information is locked away when the office is empty.

- *Desk areas are kept as clear as possible at all times, in particular medical records /other patient identifiable information /confidential documents are not held on the desk or within reach/sight of visitors.*

  Yes ✓

Information Governance Training, Policies and Procedures

- *Staff have completed Information Governance Training within the last year.*

  No X All the staff spoken to have yet to complete their annual Information Governance training. The CCG should remind staff who have yet to complete their annual Information Governance training.

- *Staff are aware of Information Governance related Policies, and know where to find them.*

  Yes ✓ Stated that they would look on the Extranet or public web site.

- *Storage, archiving and destruction of information procedures are in place.*

  No X The CSU are looking in to securing the most cost-effective offsite storage for the CCGs across Cheshire, Warrington, Wirral. The CCG should wait for this to be finalised and then consider the minimum key paper documents for offsite storage.

- *Confidential shredding procedures are in place.*

  Yes ✓ A confidential waste console unit is located in the CCG office.

Suzanne Crutchley LL.M
Senior Governance Manager (Information Governance)
Cheshire and Merseyside Commissioning Support Unit

NHS

Wirral Clinical Commissioning Group

Finance Report Month 10 – January, 2012/13 Financial Year			
Agenda Item:	3.1	**Reference:**	GB12-13/177
Report to:	Governing Body	**Meeting Date:**	5th March 2013
Lead Officer:	Mark Bakewell		
Contributors:			
Governance:	**Link to Commissioning Strategy**	Sound financial control is essential to the CCG strategy and is directly linked to the delivery of the CCG Commissioning and Operational Plan for the financial year.	
	Link to current governing body Objectives	To achieve financial control total with sound financial management.	
Summary:	This report updates the CCG on the financial performance against budgeted allocation for 2012/13 as at Month 10 (January) 2013		
Recommendation:	**To Approve**		✓
	To Note		
	Comments		
Next Steps:	Continuation of performance monitoring through the remainder of the financial year		

*This section is an assessment of the **impact** of the proposal/item. As such, it identifies the significant risks, issues and exceptions against the identified areas. Each area must contain sufficient (written in full sentences) but succinct information to allow the Board to make informed decisions. It should also make reference to the impact on the proposal/item if the Board rejects the recommended decision.*

What are the implications for the following (please state if not applicable):	
Financial	The report sets out the financial performance within the CCG for 2012/13 financial year
Value For Money	All expenditure plans are subject to an ongoing value for money review
Risk	The report details the key financial risks for the financial year and these will be monitored in year as part of the reporting process
Legal	Legal advice is sought on financial issues as and when required.
Workforce	The financial plan includes budgeted "running costs" expenditure and is reflective of the respective workforce implications in these areas
Equality & Human Rights	Financial Plans will consider as appropriate the equality impact assessment for proposals within the budgeted expenditure
Patient and Public Involvement (PPI)	Budgets include funding to ensure continued involvement of patients and public in CCG decisions.

Partnership Working	The CCG works with a number of NHS Trusts and the Local Authority on a number of its commissioning budgets.
Performance Indicators	The plan reflects the planned achievement of statutory financial duties.
Do you agree that this document can be published on the website? *(If not, please note that it may still be subject to disclosure under Freedom of Information - Freedom of Information Exemptions*	

This section gives details not only of where the actual paper has previously been submitted and what the outcome was but also of its development path ie. other papers that are directly related to the current paper under discussion.

Report History/Development Path				
Report Name	**Reference**	**Submitted to**	**Date**	**Brief Summary of Outcome**
Financial Plan		Governing Body	8th May 2012	

Private Business

The Board may exclude the public from a meeting whenever publicity (on the item under discussion) would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted or for other special reasons stated in the resolution. If this applied, items must be submitted to the private business section of the Board (Section 1 (2) Public Bodies (Admission to Meetings) Act 1960).

The definition of "prejudicial" is where the information is of a type the publication of which may be inappropriate or damaging to an identifiable person or organisation or otherwise contrary to the public interest or which relates to the provision of legal advice (for example clinical care information or employment details of an identifiable individual or commercially confidential information relating to a private sector organisation).

If a report is deemed to be for private business, please note that the tick in the box, indicating whether it can be published on the website, must be changed to a x.

If you require any additional information please contact the Lead Director/Officer.

Wirral Clinical Commissioning Group

NHS Wirral Clinical Commissioning Group

Finance Report for the period 1st April 2012 to 31st January 2013

Introduction

1. This report sets out the financial position for NHS Wirral Clinical Commissioning Group (Wirral CCG) as at the end of January (Month 10) within the 2012/13 financial year.

Resources

2. The total budget allocated to Wirral CCG for the year is £467 million from within the overall PCT baseline of £660 million. Based on the federated model approach a number of budgets are aligned to the Governing Body (£135m) to be managed on an economy wide basis and the remaining budgets devolved to the combined consortia (£332m). This is usually where practice level information is available and performance is based on actual activity (using GP Registration for individual patients).

Financial performance

3. As at the end of January (Month 10) the year to date position for Wirral CCG is an over spend of £0.5m with over performance against commissioning expenditure of £1.1m offset by an under performance against running costs of £0.6m

4. This compares to the December Month 9 position of £1.05m overspend, with the overall favourable movement of £0.6m being mainly due to further under spends on prescribing budgets, continued release of contingency reserves and further release of earmarked reserves offsetting over performance on the Wirral University Teaching Hospitals FT contract (WUTH).

5. The year to date variance position between Governing Body and the combined consortia is a overspend at divisional level of £5.45m with the Governing Body underspent by £4.99m.

6. A year to date overall Financial Summary for Wirral CCG is available in Appendix 1. The table below shows the performance variances at month 10:

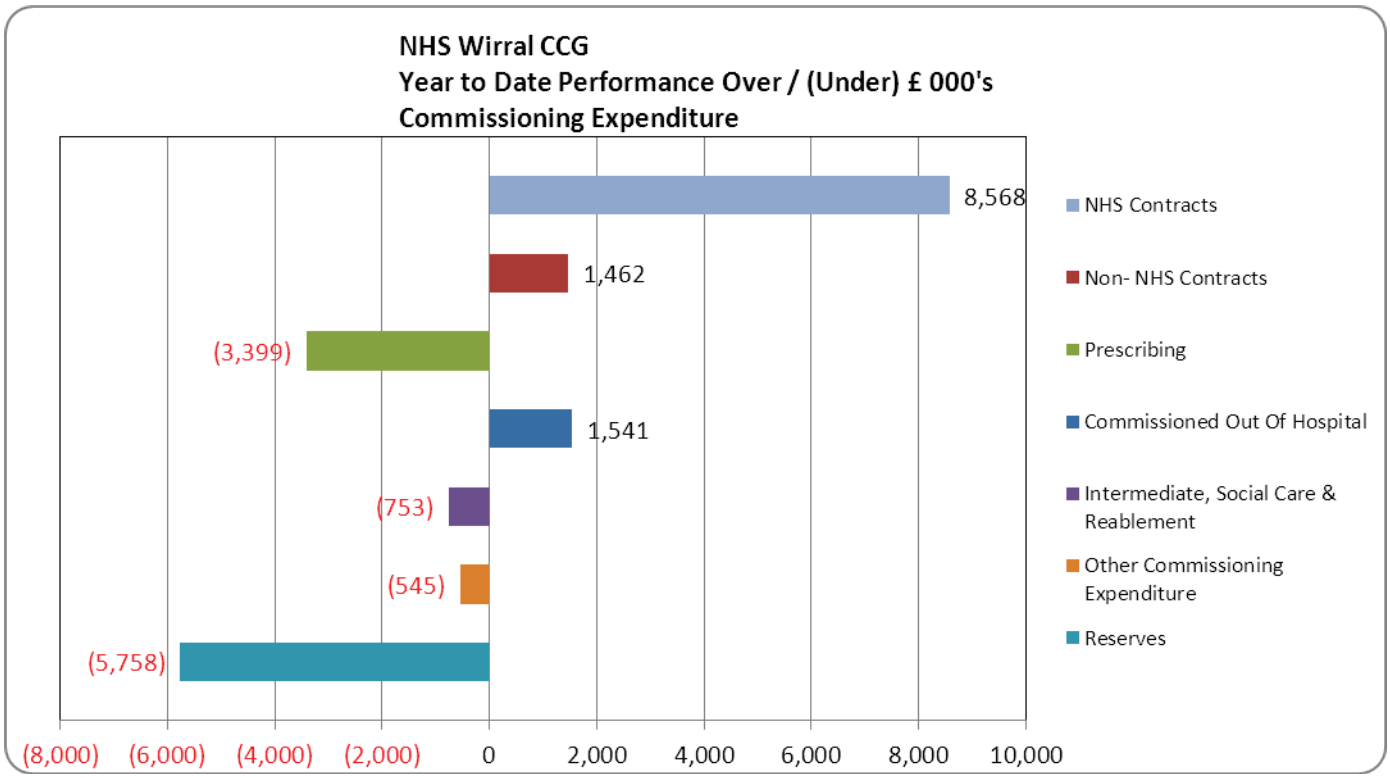
YTD variance	Combined Consortia £ 000	Governing Body £ 000	Total Wirral CCG £000
Commissioning Expenditure	5,846	(4,731)	1,115
Running costs	(372)	(261)	(632)
TOTAL	**5,474**	**(4,992)**	**482**

7. Appendix 2 shows the Divisonal Financial Summary including a summary for each of the consortia. The performance variance year to date for the consortia is shown in the table below:

YTD variance	WGPCC £ 000	WHCC £ 000	WACC £ 000	Total Wirral CCG £000
Commissioning Expenditure	(589)	6,824	(338)	5,846
Running costs	(208)	(104)	(60)	(372)
TOTAL	**(798)**	**6,721**	**(397)**	**5,474**

8. Narrative regarding financial performance is reported on an exception basis according to variation against planned levels of expenditure. More detailed information is included in Appendices 3 to 6.

9. Year to date variance from budget for the CCG is analysed below:



NHS Contracts

10. The overall CCG performance position in relation to NHS contracts shows an overspend at month 10 of £8.6m (previous month £8.1m) primarily being due to over performance on the Wirral University Teaching Hospitals NHS Foundation Trust (WUTH) contract of £7.64m (previous month £7.39m) at divisional level.

11. The year to date position is based on actual activity as at Month 9 (as per table below) £6.9m over performance with a pro-rata adjustment to equate to month 10 position and application of estimated contract adjustments for re-admissions / outpatient follow-up ratios as appropriate (again based on the month 9 actual activity position).

WUTH Point of Delivery	YTD Actual Performance as at M6 Sept 2012 Over / (Under) £ 000's	YTD Actual Performance as at M7 Oct 2012 Over / (Under) £ 000's	YTD Actual Performance as at M8 Nov 2012 Over / (Under) £ 000's	YTD Actual Performance as at M9 Dec 2012 Over / (Under) £ 000's
Elective	917	1,223	1,446	1,698
Non-Elective	1,446	2,044	2,449	2,727
Outpatient Attendances	831	1,084	1,156	1,151
Outpatient Procedures	562	696	802	865
A&E	(4)	(13)	34	62
PbR Total	**3,752**	**5,034**	**5,887**	**6,503**
Non-PbR Total	408	550	772	471

POD Total	4,160	5,584	6,659	6,974

12. The point of delivery above shows over performance across the majority of areas. Non-elective performance has been fixed at an agreed outturn level and pro-rata is in line with year to date position, elective point of delivery over performance has increased which was expected due to the referral trends from earlier in the year.

13. There has been a reduction in the run rate of the in-month overspend between months 8 and 9 which would support the view that work streams led by the CCG are beginning to have some positive effects (practice visits / referral pattern etc)

14. Performance on other NHS contracts shows a combined overspend of £929k year to date (previous month £727k) with the over performance on the Royal Liverpool and Broad green University Hospital contract currently £298k year to date (due to high cost drugs) but it is anticipated that this overspend will be reduced once in month 11 reporting once further clarity is provided on the commissioner's agreement with Mersey trusts is factored into the position regarding the fixed outturn position

15. There is also over performance year to date on the North West Ambulance Service contract of £183k, Warrington and Halton Hospital £59k, and Countess of Chester £59k.

Non-NHS Contracts

16. At month 9 Non NHS Contracts are over spent to date by £1.46m (previous month £1.28m).

17. With the utilisation of the two AQP's radiology and physiotherapy, it is anticipated that under performance will be seen in other areas to compensate the reported expenditure. Other existing performance factors are outlined below.

18. Firstly the backlog of patients transferring to "Spire" due to 18 week RTT targets from earlier in the financial year of £209k. Specialist Care (Health Treatment Panel) is also overspent £85k.

19. Over performance against planned levels of activity also exist and continue against the Independent Midwifery One to One provider £461k for ante / post natal care, Spa Medica (Ophthalmology Cataracts) £327k, and the "Spire" contract for patient choice referrals (non RTT Backlog patients) £154k.

20. Under performance continues on the Assura Ophthalmology contract £104k year to date and also in Primary Care Mental Health contracts £414k year to date.

Prescribing

21. Prescribing expenditure is currently providing the CCG with a year to date underspend of £3.4m (previous month £2.96m). There is an under performance of those budgets managed at Governing Body level of £377k and underperformance at divisional level of £3.02m. The performance position is based on eight month's actual data with two months estimated costs for December and January.

22. The year to date divisional underspend is primarily due to cost growth, a substantial drop in generic drug prices and the delay in the transfer of prescribing dementia drugs to primary care and underperformance in respect of planned drug developments as per the original financial plan.

Commissioned Out of Hospital

23. Commissioned "out of hospital" budgets are £1.54m overspent at month 10, an adverse in month movement of £114k. The main drivers for the continued over performance remain within the Continuing Healthcare section with Older People (£244k), Mental Health (£347k) and Physical Disabilities (£275k), and all Joint Funded packages (£899k) These overspends are being partially offset by underperformance on Funded Registered Nursing Care (FRNC) of (-£295)k.

Reserves

24. Reserves are underspent by £5.76m at Month 10 which is due to the release of the contingency element and a number of earmarked reserves which are available for release.

Running Costs

25. There is a year to date underspend of £632k in relation to running costs at month 10, an adverse in month movement of £64k. This is primarily due to the movement in under performance on the Commissioning Support Unit (CSU) costs at Governing Body level £421k (previous month £445k). Clinical backfill reported at consortia level continues to underperform year to date (£297k). A review with the individual consortia leads is on-going to ensure all approved expenditure is being captured within the position.

Forecast Outturn

26. Based on the information received as at month 10 within the 2012/13 financial year (January), the position for the CCG remains on track to achieve a balanced position against it delegated budget and from an overall perspective the PCT is still in a position to achieve its overall control total

27. One of the key performance drivers to the financial performance position remains around the WUTH contract and intelligence regarding contract performance using the month 9 position resulted in a stable forecast outturn position to the value of £9.0m

28. There have been minimal movements in the other sections of the CCG's expenditure however prescribing continues to provide a material underperformance against planned expenditure (£4.3m)

29. As per Month 9 QPF reporting position, the movement in other commissioning is based on the review of consortia commitments in order to reduce overall expenditure within the CCG position

30. Management of the year end position given the current assumptions would be set out as per the below:

NHS Wirral Clinical Commissioning Group Financial Summary - 2012/13				
Month 10	**Annual Budget**	**Forecast Variance M10**	**Forecast Variance M9**	**move-ment**
Clinical Commissioning Groups(CCG)	£'000	£'000	£'000	£'000
NHS Contracts	329,902	10,081	9,977	104
Non-NHS Contracts	12,565	1,806	1,721	84
Prescribing	59,815	(4,378)	(4,110)	(268)
Commissioned Out of Hospital	29,399	1,842	1,937	(95)
Intermediate, Social Care & Reablement	8,900	(902)	(926)	24
Other Commissioning Expenditure	8,623	(720)	(55)	(664)
Reserves	7,635	(7,006)	(7,025)	19
Cost Improvement Programme	0	0	0	0
Total CCG Commissioning Expenditure	**456,838**	**723**	**1,520**	**(796)**
Running Costs	**9,829**	(724)	(845)	121
Overall CCG	**466,667**	**(0)**	**674**	**(675)**

Financial Risk

31. The CCG's Financial Plans identified the main areas of financial risk in terms of performance for the year and an overall CCG Risk with regards to financial performance.

Original Risk Identified	Potential Risk Value	Degree of Forecast Risk	Current Forecast Performance	Degree of Forecast Risk
Commissioned Out of Hospital	£1.0 million		£1.9m	
Performance on Secondary Care Contracts (WUTH)	£3.0 million		£9.0m	
Prescribing	£1.2 million		(£4.3m)	
Cost Efficiencies	£6.2 million		Linked to other risks as embedded within contracts but managed via contingency	

Degree of Forecast Risk – Assessed as

Red Over performance > 2%
Amber Over performance > 1% or risk of delivery
Green Minimal Risk (Forecast Underperformance or low value)

32. Risks will be subject to constant review as more information becomes available regarding performance against planned levels of expenditure.

Conclusion

33. Wirral CCG's Governing Body is asked to note:

- the financial position as at the end of January 2012
- the forecast outturn position for 2012/13

Mark Bakewell
Chief Financial Officer
NHS Wirral Clinical Commissioning Group

20th February 2013

Wirral GP Commissioning Consortium

NHS
Wirral Clinical Commissioning Group

WIRRAL GP COMMISSIONING CONSORTIUM
EXECUTIVE BOARD MEETING
Minutes of Meeting

Tuesday 15th January 2013, 7pm
Nightingale Room, Old Market House

Present:

Dr Akhtar Ali	(AA)	GP Lead
Christine Campbell	(CC)	Chief Officer (Acting) (Chair)
Chandra Dodgson	(CDo)	Finance Lead
Dr Denyse Kershaw	(DK)	GP Lead
Dr Hannah McKay	(HM)	GP Lead
Dr Abhi Mantgani	(AM)	Clinical Chief Officer – Wirral CCG
Dr John Oates	(JO)	Chair
Ann Riley	(AR)	Nurse Member
Eddy Shallcross	(ES)	Patient Council Chair
Dr Pankaj Srivastava	(PS)	GP Lead

In attendance:

Anita Fletcher	(AF)	WGPCC Administrator
Kerry Hogan	(KH)	Commissioning & Engagement Support Manager
Paul McGovern	(PM)	Commissioning Support Manager
Jill Quayle	(JQ)	Foundation Years Trust

Ref No.	Minute
WGPCC/EB/ 12-13/0070	**1.1 Apologies for absence** Apologies were received from Dr Navaid Alam, Karen Hornby and Lysa Morton
	1.2 Declarations of interest No declarations of interest were made.
	1.3 Public Comments/Questions There were no members of the public present.
	1.4 Minutes and Action Points of the last meeting The minutes from the last meeting were agreed to be a true record of the meeting. <u>Matters Arising</u> **Primary Care Mental Health Progress Report** – Members were advised that a meeting had only taken place the day Board papers were issued, therefore a full update would be given at the February Board meeting. Members were informed that 95% of patients were being seen within 20 working days, although there was still a major issue around figures and waiting times, and around the interpretation of whether the target records waiting time to assessment, or waiting time to therapy. The Regional IAPT team has agreed to meet with KH to take forward. An email will be sent to practices requesting individual issues or concerns that will feed into this

Ref No.	Minute
	review. The Consortium has been working closely with the provider to maintain the triage and assessment step, and to explore if there are any issues with the pathway contributing to the long waiting times. It was explained that Peninsula is receiving the same number of referrals proportional to its practices' patient populations as the other WGPCC primary care mental health providers. No further investment will be made until the Consortium is satisfied that any operational issues with the provider have been addressed. Members would like information on the length of waiting time for the longest waiting patient, for Steps 3 and 4. It was confirmed that there are no similar concerns with the other service providers. Practices are able to change providers, but must give six months' notice if they wish to change alternatively an agreed timescale between both parties can be met. Any practices who have issues with the service should contact KH. A full update of the service will be provided at the next Executive Board meeting. **Proposal for Investing in the Foundation Years Trust Pilot Project to Improve Life Chances of Local Children** – This paper had been presented at the December meeting of the Executive Board, and members had requested further information before being able to support the proposal. Gill Quayle from the Trust gave further background to Executive Board Members. She highlighted the three aims for the project – better access to services, confident parents and on-going support through volunteers. Some people have better access to services than others and this should be the same across the board. It was felt education for parents is essential so it was decided to tackle this at the ante-natal stage. The funding sought is to pump-prime the project and enable it to be properly managed and evaluated. The project will be focused on patients within the WGPCC practice area and so the Consortium will be able to benefit from the learning and the health benefits. Members were advised that Tranmere/Rock Ferry were chosen due to the patient demographic. This is a pilot, and so would be rolled out to other areas if successful. The pilot is working with 30 families with a first child. The pilot would take six months to test the model, then taking into account the initial evaluation, enrolling 100 families for the full project. The project fits in well with Homestart; when parents are identified, they will be linked with a Homestart volunteer for the first 12 months. Members were concerned that evaluation would not take place until the children started school, therefore 4 / 5 years post-implementation. It was felt that there might be specific health matters that could be measured, for example immunisation rates. Gill agreed that clearly defined health parameters would have to be looked at. Members were informed that the pilot project was almost up and running, funds had been made available for this by the Local Authority; the money requested would be for the whole project not just for the pilot. Gill Quayle was thanked for updating members and was advised that she would be notified of the Board's decision in due course. <u>Action Points</u> Clinical Education Lead – It was confirmed that a letter had been issued to Dr Lee to advise him of Dr Alam taking the role as WGPCC Education Lead, further to discussion at the last meeting. Clinical Geneticist – Members were advised that a GP at Liverpool Hospital had been in contact with Dr Srivastava regarding training to GPs. It was asked that details of this should be

Ref No.	Minute
	forwarded to KH. Proposal for Investing in the Foundation Years Trust Pilot Project to Improve Life Chances of Local Children – AM explained that he had an indirect interest in this matter, as he had been invited by the Chair of the Trust to sit on the Board but had not attended meetings for some time. The Chair did not consider this interest to be sufficiently material to prevent AM from participating in the decision-making process. Following discussion around the proposal, members were in support of investing the £100,000 necessary, but with the caveat that the Consortium needs to be able to influence the project's metrics and to receive regular reports. The Chief Officer would finalise details with the service provider. Executive Board Members were happy to support this proposal, based on the direct benefit to WGPCC patients and the learning that could be gained and rolled out within other projects, and make the investment of £100,000 to support this.
	1.5 Minutes for Noting Executive Board Members noted the minutes of the Wirral Clinical Commissioning Group Governing Body meeting which was held on 4th December 2012.
WGPCC/EB/ 12-13/0071	**2.1 Local Authority Budget Options** Members were advised that Public Health had produced a paper on the implications of the Local Authority budget option proposals. The document had not yet been circulated publicly. The Local Authority has to make savings of £100 million over the next three years in areas of health, social care and recreational. Each Consortium has been asked to comment on the proposals and give a view on areas that have implications for health and wellbeing. The paper will be circulated in due course and comments will be sought. Some items that are agreed on now without impact may have long term effects on the population. Wirral Council have advised that this will impact on services but they do not have a choice in the matter. The consultation process is due to conclude on 31st January 2013; Members were asked to forward any comments to KH to collate so that these may form part of the Wirral CCG response.
	2.2 WGPCC Terms of Reference Members were advised that the document had been due for review in December 2012 but it had been agreed to review in time for the new financial year. Each Consortium's terms of reference needs to be consistent in terms of arrangements for practices transferring between consortia, and quoracy requirements, and each needs to fit in with the CCG Constitution. CC is to make proposed amendments to the current terms of reference, taking the above into account, and Board members were requested to provide their feedback once these are circulated. The areas changed will be highlighted. The quorum section is extremely important to review, as decision making ability has been affected when meetings are not quorate. Some areas have changed during the year, for example Secondary Care representation. The Consortium would like to see extra patient representatives on the Board. The current WGPCC constitution will be amalgamated into the terms of reference, as there will only be one Wirral-wide constitution. **Action:** CC to circulate revised terms of reference for comment.

Ref No.	Minute
	2.3 Wirral CCG Constitution Members were advised that a draft constitution had been circulated to Stakeholders for comments. The Wirral CCG Governing Body had reviewed and accepted the comments received where appropriate. It was envisaged that the amended version of the document would be issued to practices shortly; final comments will be brought back to the Governing Body for final approval. Once this has been completed, the Constitution will be issued to practices for signing. Changes – Members were informed that, due to Drs Jennings and Mantgani attending the Board with a Wirral-wide role, rather than representing their consortia, additional representation from WHCC and WGPCC at Board meetings will need to be sought; once approved this will be included in the Terms of Reference. Delegation – The level of delegation to between the CCG and Consortia needs to be agreed. An impact assessment tool has been developed and will determine which decisions can be made at a Consortium-level, and what must be taken for Governing body review. LMC representation on the Governing Body Board had been requested again by the LMC, and members were advised that this had been discussed by the Governing Body, and the Consortia Boards, on three separate occasions, and the consensus remains that it was felt not appropriate for anyone from a representative body, including the LMC, to have a seat on the Board.
WGPCC/EB/ 12-13/0072	**3.1 Financial Budget 2012/13** Executive Board Members were advised that as at the end of November 2012 (Month 8) the Consortium was overspent by £30,000 which was an improvement in the position of £114,000 on the previous month. This is mainly due to the reduction in the over performance on other commissioning expenditure. With regard to concerns raised around the Physiotherapy AQP, members were advised that this was still not accurate in Month 8 position and would be adjusted in Month 9. The year to date position for Wirral CCG is an overspend of £1,083k with a balanced budget being forecast by year end. With regards to invoices, practices have been advised to submit these as soon as possible to release funds. However, where a practice will not be able to spend a resource committed to them before the end of March 2013, this resource should be put on hold to support the CCG bottom line, with a guarantee that the resource will be recommitted in April 2013. Non-recurring monies will be available next year and a formula will be implemented for practices. **Action:** CD to identify practice bids where resources could be pulled back to support the CCG bottom line. Congratulations were given to the Consortium practices for continuing to work hard to maintain a near underspent position. Overspend practices were being worked with. AM requested that expenditure in locally commissioned services is described alongside what the cost to the Consortium would have been, should the activity have been undertaken elsewhere at a full tariff price. **Action:** CDo to change the presentation of this section of the report.

Ref No.	Minute
	3.2 Patient Council and Engagement Update Following a long illness, ES was welcomed back to the Executive Board. Members were informed that patients were invited to attend a workshop to discuss a DNA reduction campaign that has been designed following feedback from the Patient Council. A focus group was held to test out messages with patients. A poster and flyer have been developed to emphasise key messages. An appointment card which will be credit card size has been created to remind patients of their appointments. The intention is for a patient to write down their own appointment details to take ownership. The card will feature details of the Choose Well campaign, to highlight alternatives to A&E such as the Minor Injury and Illness services.. It had been suggested for a stack of cards to be given to patients in order for them to be kept at home. Posters will be displayed in pharmacies and libraries to target those that do not attend their practice; the campaign which will be launched in February and will include a press campaign. The question was raised as to why patients do not attend; a focus group will be put together to ask patients for feedback on why they have missed appointments. Data will be gathered from practices and good practice where there are low DNA rates will be shared with all. Members were advised that an evaluation of the DNA campaign will take place in September.
	3.3 Executive Nurse Update Members were advised that the Nurse Training Programme is due to be launched on Wednesday 16th January 2013. A full year's training programme has been put together based on consultation with nurses and practice managers. Meetings have taken place with various pharmaceutical representatives who will be funding some of the training. Feedback so far has been really positive. The programme will be emailed out to Practice Nurses, Practice Managers and Clinical Leads.
	3.4 Practice Manager Update No update was available as KH and LM were not present at the meeting.
	3.5 Items for Risk Register There were no items for the risk register.
WGPCC/EB/ 12-13/0073	**5. Any Other Business** CC explained that KH, CD and PM were meeting to look at commissioning priorities for WGPCC for 2013/14, based on practice and patient feedback, activity and evidence such as the JSNA. These discussions will take into account the need to comply with contractual deadlines regarding embedding commissioning intentions within the main provider contracts. It was agreed that the Consortium will work with other Consortia wherever this makes sense to do so, but will continue to develop commissioning intentions and projects that are unique to the needs of our population, and reserve the right to flex Wirral-wide projects and service models in line with our population's and practices' needs.
WGPCC/EB/ 12-13/0074	**6. Private Business** This section was discussed as private business.

Ref No.	Minute
	7. Date and Time of Next Meeting The date and time of the next meeting is Tuesday 12th February 2013, 7.00pm in the Nightingale Room, Old Market House, Birkenhead. Please send any apologies to Anita Fletcher on anita.fletcher@wirral.nhs.uk

The meeting finished at 9.15 pm

Wirral Clinical Commissioning Group

WIRRAL HEALTH COMMISSIONING CONSORTIUM
EXECUTIVE COMMITTEE
Minutes of Meeting

Wednesday 16th January 2013
Albert Lodge - Victoria Central Health Centre

Present:	Dr Pete Naylor (Chair)	Chair
	Mr Andrew Cooper	Chief Officer
	Dr Paula Cowan	GP Executive Lead
	Dr David Jones	GP Executive Lead
	Dr Sue Kidd	GP Executive Lead
	Dr Sean Magennis	GP Executive Lead
	Dr Sue Wells	GP Executive Lead
	Louise Morris	Finance Lead
	Brian Knight	Patient Forum Representative
	Carol Heath	Practice Nurse Representative
	Anita Swift	Practice Manager Representative

In Attendance:

Pauline Bolt	Commissioning Support Manager
Wendy Holmes	Executive Assistant

Ref No	Minute
WHCC/EB/ 12-13/0091	**1.1 Apologies for Absence** Apologies were received from Dr Shyamal Mukherjee, Graham Hodkinson and Councillor Phil Davies.
WHCC/EB/ 12-13/0092	**1.2 Declarations of Interest** Declarations of interest were made for item 3.1 Phlebotomy Specification Review by the GP Executive Leads.
WHCC/EB/ 12-13/0093	**1.3 Public Comments/Questions** There were no members of the public in attendance.
WHCC/EB/ 12-13/0094	**1.4 Minutes from the last meeting** The minutes from the previous meeting were reviewed and accepted as an accurate reflection. <u>Matters Arising</u> An update on BME paper from Commissioning Support Manager (Laura Thompson) required.

Ref No	Minute
	Actions The ICE Programme Board has commenced and a presentation will be given at GP Members Committee. Telehealth Service – Chief Officer to confirm that the service was raised at Practice Nurse Forum. Admission Avoidance Service template has been produced for the main service providers over the last 12 months. Approximately 150 patients have accessed the service. The template will be updated as soon as possible and will be presented to the Business Development Group. Practice Leaflets – the leaflet is ready to be sent out with a very brief survey. The provider has agreed to collate survey responses, providing that the questions require simple Yes/No answers. The Patient Representative agreed to speak to the Patient Forum regarding the survey. Two mock up versions of the leaflet were circulated for comments. Feedback on the layout was noted by the Commissioning Support Manager. It was confirmed that the LT Print quote received is definitely a quote and not an estimate. MediDoc will insert the leaflets into envelopes with a covering letter and use a PO Box number for despatching and collating returns. Postage will need to be paid for returned envelopes. The costings were advised as £53,470.68. The standard box of foreign language text will be included in the leaflet. Additional costs of printing leaflets by specific language will be on a case by case basis. The text will also be included on the patient survey (on the reverse side of the covering letter). The Commissioning Support Manager will contact each practice for their individual opening hours. It was agreed that the wording on the leaflet regarding A&E costs should state "up to" £250. As discussed at the last meeting, practices will have the option to opt out of having a new leaflet produced if they prefer to continue with their own version. ***Action*** *- Service Review to be added to agenda for next meeting (Executive Assistant)*
WHCC/EB/ 12-13/0095	**2.1 Dementia and End of Life Education** The Commissioning Support Manager presented a proposal paper for Dementia and End of Life education for Care Home staff, following feedback received from the Falls Workshop. Costs are based on the Falls Workshop of £1244.40 for venue, refreshments and equipment. An additional £450 would be required to extend the contract of the agency admin support officer for a further week to arrange the event. The services that will be invited to present at the event will include Alzheimer's Society, Memory Clinic and Medicines Management, amongst others. It was queried whether it would be of benefit to liaise with Brimstage Manor regarding good practice for dementia care. The Commissioning Support Manager agreed to look at

Ref No	Minute
	this. The Chief Officer asked that the Board approve the additional admin support costs due to limited capacity available. It is proposed that the Wirral wide event would take place early to mid March. Wirral GP Commissioning Consortium (WGPCC) has agreed to share costs and it is expected that Wirral Alliance Commissioning Consortium (WACC) will also agree. The Board approved the proposal. ***Action*** *– Commissioning Support Manager to contact Brimstage Manor regarding sharing dementia care good practice.*
WHCC/EB/ 12-13/0096	**3.1 Phlebotomy Specification Review** The Commissioning Support Manager advised that the current service was awarded to Wirral Community Trust in October 2008 and subsequently extended to October 2013. It is a block contract which has an activity cap. Interventions are charged at cost per case over and above the cap. Feedback received from practices and the service provider was outlined in the report (paragraphs 15 and 16). The number of appointments available by practice and the number of appointments not utilised, was brought to the attention of the Board. The percentage figure of appointments not used included DNAs. It was noted that there are a lot of spare appointments and capacity needs to be managed more effectively. As the current contract is due to expire in October, future options for the way forward need to be investigated. It was advised that the paper has already been discussed by the Wirral CCG Operational Team. The Commissioning Support Manager is organising for Task and Finish Groups to look at specific issues that have been identified, acknowledging that not all issues will be resolved. The Task and Finish Groups will require a GP representative from each division. Practices are likely to have an option to opt out of the Wirral wide service and it is proposed that the service specification may need to be split into a domiciliary service and an appointment service. Costings for the service will need to be reviewed as part of the process and consideration needs to be taken of how resource will be apportioned back to practices should they wish to opt out of the Wirral service. A discussion followed on advantages of hubs for patients to attend and a centralised booking service. Issues of patients attending clinics without the relevant paperwork were highlighted. It was agreed that there would need to be two working groups to look at this piece of

Ref No	Minute
	work. Comments/suggestions should be emailed to the Commissioning Support Manager to take forward with working groups. ***Action*** *– Chief Officer to email practices requesting GP representative for Task and Finish Group.*
WHCC/EB/ 12-13/0097	**4.1 Finance Update** The finance report as at the end of Month 8 (November 2012) was reviewed by the Board. WHCC is overspent by £5.6m (£3.84m previous month overspend). The consortium worsened during the month by £1.8m (previous month £459k). NHS contracts overspent £5.9m. At point of delivery level the performance at WUTH remains as a result of over performance in planned care (Elective and Outpatient) and Non-Elective and underperformance in Non-elective – non emergency and Accident and Emergency attendances. The breakdown figures were outlined in paragraph 6 of the report. The variance between October and November for Non PbR in Month 8 was illustrated in the table in paragraph 8 of the report. Actuals by practice are now available. Non-NHS Contracts is £580k overspent – main drivers were advised as Spire and Spa Medica. Prescribing continues to show an underspend position of £474k, an improvement of £63k. Other Commissioning shows underspend of £296k. Running Costs continue underspend position (£102k), mainly due to clinical backfill. Consortium investment spend to date is £634k and budget of £311k has been transferred to support the Hospice at Home service and Primary Care Mental Health - totalling £828k. Forecast outturn is a potential overspend of £7.41m (£6.19m last month) for the consortium. The consortium must submit spending plans by end of February for this financial year. A paper was circulated for information outlining spend by division. In summary, WGPCC are 1% over budget and WACC are 2% over budget. A discussion followed on GP referrals and the need to understand the significant change in figures. Wirral CCG is in an unbalanced position, currently forecasting £600-£800k overspend.
WHCC/EB/ 12-13/0098	**4.2 Items for Risk Log**

Ref No	Minute
	Risk Log to be reviewed and updated to reflect overspend position.
WHCC/EB/ 12-13/0099	**4.3 Risk Register** No comments were received.
WHCC/EB/ 12-13/0100	**5.1 Subgroup Minutes for Noting** The minutes from the November meetings of the sub-committees were noted.
WHCC/EB/ 12-13/0101	**6. Summary of Actions** Please refer to action points attached.
WHCC/EB/ 12-13/0102	**7. Summary of Financial Approvals** Amended Practice Leaflets and Dementia Workshop costs to be added to summary sheet.
WHCC/EB/ 12-13/0103	**8. Any Other Business** The Finance Lead advised that she had been appointed as Finance representative for Wirral CCG and will therefore cover all divisions. The Board congratulated Louise on her appointment and wished her well for her forthcoming maternity leave. It was noted that Emma Shanks will be covering maternity leave.
	Date and Time of Next Meeting The date and time of the next meeting is Wednesday 20th February 2013, 1.00pm at Albert Lodge, Victoria Central Health Centre. Apologies have been received from the Practice Manager Representative. Please send any other apologies to Wendy Holmes on wendy.holmes@wirral.nhs.uk

WIRRAL ALLIANCE COMMISSIONING CONSORTIUM
EXECUTIVE BOARD MEETING
Minutes of Meeting

Thursday 10th January 2013
Old Market House, Wirral

Present:

Dr Mark Green (Chair)	St Hilary Group Practice
Dr Helen Downs	Civic Medical Centre
Dr Gillian Francis	Spital Surgery
Dr M Salahuddin	Gladstone Medical Centre
Dr Richard Williams	Riverside Surgery
Dr Ivan Camphor	Heatherlands Medical Centre
Iain Stewart	Chief Officer
Michael Roach	Non-Executive Advisor

In Attendance:

Allison Hayes	Executive Assistant
Sheena Wood	Commissioning Manager
Paul Wormald	Strategic Information Analyst
Louise Morris	Finance Link, CWW CSU
Allan Stewart	Practice Manager Representative
Dr James Kingsland	Strategic Development Lead
Julie Webster	Deputy Head of Public Health
Mr L Clearkin	Consultant Ophthalmologist

Ref No.	Minute
WACC/EB/ 12-13/0037	**Presentation by Dr Louis Clearkin** Mr Clearkin gave a presentation to group members regarding Tear Film Instability and how a website can aid GPs and patients in managing the condition. Members were asked to consider piloting the scheme for 3 months. Members agreed. ***Action*** **–** Chief Officer, Chair and Commissioning Manager to meet with Mr Clearkin to discuss the progression of the pilot. **Preliminary Business** **1.1 Apologies for absence** Apologies were received from Dr Bryan Conlan and Fiona Johnstone.
	1.2 Declarations of interest There were no declarations of interest declared. **1.3 Minutes and Action Points of Previous Meeting/Matters Arising** The minutes from the previous meeting held on 6th December 2012 were agreed as a true record of the meeting and were proposed by Dr Downs and seconded by Dr Francis. Chief Officer updated the group with regards to the District Nursing Service and informed members that their issues and concerns have been raised with the provider.

Ref No.	Minute
	Action Points – Please refer to the attached sheet. **1.4 Chair Report** **Governing Body Update** The Chair provided the group with an update with regards to the recent site visit regarding authorisation and the progress of the CCG constitution. An update on patient engagement to support wider recruitment of patient involvement at both practice level and consortia level was given and the details of a leaflet for patients to complete within their practices. Chair informed the group of the A&E waiting time performance at WUTH. Chair informed members of paper which is to be produced and submitted to practices in order for them to make their comments regarding a review of the Phlebotomy service.
WACC/EB/ 12-13/0038	**Items for Discussion** **2.1 Authorisation Feedback** A discussion took place on the role of Wirral Local Medical Committee (LMC) and its involvement in the CCG Governing Body. GP Member stated that the LMC wanted to achieve better engagement with the Governing Body. Chair reiterated that LMC representation within the CCG Governing Body was a matter for those two statutory organisations to conclude and not consortium core business. **2.2 Commissioning Plan** Members briefly discussed future commissioning plan ideas and agreed for this to be discussed further at the next Clinical Working Group meeting in February. **2.3 Board Development/Open Meetings** Chair informed the group of the requirement to hold consortium board meetings in public with effect from April 2013 and that further development on board etiquette will be implemented.
WACC/EB/ 12-13/0039	**Items for Approval** **3.1 Practice Proposals** **Advanced Nurse Practitioner and Informatics Update** Commissioning Manager sought approval for the two proposals recommended by the Clinical Working Group – members agreed to progress proposals. ***Action*** – Commissioning Manager to progress with proposals.
WACC/EB/ 12-13/0040	**Items for Information** **4.1 Quality, Performance and Finance** Strategic Information Analyst provided an update to the Board. Specific analysis on referrals trend over last 4 years showed a continuing downward trend across the consortium. Members discussed the need for dermatology up-skilling options. ***Action*** – Commissioning Manager to review Dermatology up-skilling options and feedback to future meeting. **Finance** Finance member provided the Board with an update based on month 8 performance forecast for month 9. Overall the consortium is currently forecasting a small underspend position as at end of March 2013.

Ref No.	Minute
	Board members were asked to note: • The financial position as at the end of November 2012 • The forecast outturn position for 2012/13 financial year • The requirement for the consortium to implement spending plans as soon as possible • The potential risks identified for 2012/13 financial performance Member discussed AQP for Cataracts and this is to be an agenda item for a future CWG meeting. ***Action –*** Commissioning Manager to review current status for AQP for Cataracts provision. **4.2 Risk Register** • No new risks identified.
WACC/EB/ 12-13/0041	**5.0 Subcommittees minutes for noting** The minutes from the subcommittees meetings were noted.
	6.0 Summary of Actions Please refer to action points attached.
	7.0 Any other Business Practice Manager Representative raised concerns regarding the restrictions on software applications available for use with the recent iPads provided by the CCG, as it is potentially rendering the devices obsolete. **Action: Chief Officer to feedback to CCG Governing body**.
	Private Business None.
	8.0 Date and Time of Next Meeting The date and time of the next meeting is ***Thursday 7th February 2013, 3pm at Civic Medical Centre, Bebington.*** Please send any apologies to Allison Hayes on allison.hayes@wirral.nhs.uk

Wirral Clinical Commissioning Group

WIRRAL CLINICAL COMMISSIONING GROUP
APPROVALS COMMITTEE
Minutes of Meeting

Friday 16th November2012
Room 539, 5th Floor, Old Market House

In Attendance:

Dr A Mantgani (AM)	Designated Accountable Officer WCCG
Simon Wagner	Lay Advisor(Patient Champion) WCCG
James Kay (JK)	Lay Advisor designate WCCG (Chair)
Lorna Quigley (LQ)	Chief Officer WCCG
Mike Roach (MR)	Non-Executive Advisor NHS Wirral
Mark Bakewell (MB)	Chief Finance Officer WCCG
Phil Davies (PD)	Non-Executive Advisor NHS Wirral
Iain Stewart (IS)	Chief Officer Wirral Alliance
John Callcott (JC)	Non-Executive Advisor- NHS Wirral
Fiona Johnstone (FJ)	Director of Public Health

REF NO.	MINUTES	ACTIONS
AC/12-13/17	**PRELIMINARY BUSINESS**	
	Apologies for absence Apologies for absence for Andrew Cooper , Christine Campbell **Actions from Previous Meeting** The minutes where recorded and signed as a true and accurate record.	
AC/12-13/18	**ACTIONS FOR DISCUSSION**	
	Terms of Reference Terms of reference for the approvals committee have been approved by the Governing Body. Regular meeting dates for the committee have been arranged and circulated. The approvals committee template has been updated; however this hasn't been used universally by all consortia. Template to be sent to out to all consortia	**LQ**

REF NO.	MINUTES	ACTIONS
	Approvals Tracker An updated approval tracker has been included with the agenda. Following discussion, it was agreed that an additional 2 columns would be added to include the date proposal submitted and the date the proposal was approved. The heading would also be changed from cluster to committee.	**MB**
AC/12-13/19	**ITEMS FOR APPROVAL**	
	3.1 Activity Review The background to this proposal was presented by the Chief Clinical Officer, the CCG has seen an increase in elective and non elective activity. This proposal is a way of supporting practices to undertake an audit in order for them to gain an understanding and ownership into their practice activity. It was clarified that this with all enhanced services that this was optional, however it is anticipated that most practices would undertake this as the proposal has been supported by the Chief Officers and the Chairs of the consortia. This audit is separate to the audit requirements for QOF. Discussion took place regarding the calculation of finances to this proposal. This has been based on the work that has been undertaken in the "deep dive" exercises that have been undertaken by practices, and has been tested through the Primary Care team in terms of duplication The lay advisor (patient champion) raised potential confusion regarding the terminology of over performance to overspend. The lay advisor also queried if patients needed to know and how their opinion had been sought regarding the use of the information. It was clarified that this was an anonymised data collection process on information held at practice level. This intelligence may help to inform future contracting arrangements with provider and was to provide themes for further exploration and not patient specific The question was raised what would happen if practices didn't complete the audit satisfactorily. The Committee was assured there is an established process to claw back funding which has been implemented in the past.	

REF NO.	MINUTES	ACTIONS
	 Approval committee template - activity re\	
	The Approvals Committee approved the proposal**.**	
	NB- before this goes onto the website, the cover sheet will be altered to reflect the discussion re patient engagement.	**LQ**
	3.2 Urgent Care (4 Practices)	
	NB declaration of Interest for M Roach/Iain Stewart	
	The Chief clinical officer presented four proposals that have been submitted from the Wirral Alliance. The aim of the proposal is to pilot in four GP practices different models of delivering urgent care, in order to reduce the number of patients who attend the Accident and Emergency department with minor complaints. This would support the department in achieving the four hour target.	
	Clarification was sought regarding these proposals as to whether they should be seen as four separate proposals, or as one proposal. A single, unified proposal would exceed the delegated limit to CCG's and would need to go to approval at cluster level. The Director of Public Health commented that in past her projects have been challenged if they come under the same programme heading.	
	It was brought to the committee's attention that these proposals had been brought to the consortia board separately. It was only a matter of timing that they are now being discussed on the same approvals committee agenda. On a practical level it is also unclear now who or what committee there was in the cluster to provide such approval - due to the changes over the last 6-12 months.	
	Following these discussions the Chair sought from the Chief Clinical Officer and the Chief Finance Officer assurances that it was appropriate for the Approvals Committee to deal with them as four single projects with each falling within the £200,000 turnover limit for local approval. This assurance was given.	
	It was noted that there was some variation in costings within the four projects. This was explained to be due to the different models that are being tested by the pilots. This further emphasised the differences between the projects.	
	A concern was raised about the inclusion within a budget of 'hosting costs'. It was agreed that this would be taken out of the St Hilary Brow proposal as they are provided the services to their own patients and not hosting another organisation or practice's patients.	**IS**

REF NO.	MINUTES	ACTIONS
	The lay advisor (patient champion) asked to see the evaluation that would be used to assess the patient experience. It was agreed that the proforma would be sent to him. A question was raised about the original urgent care strategy surrounding the concept of the single front door. The committee was informed of the CCGs pending review of the urgent care strategy and the process that is being undertaken in order to arrest the rise in demand. It was acknowledged that there may be a need to pilot different models on an interim basis until the long term strategy could be implemented. The proposals were discussed and approved in the following order: • St Hiliary Brow approved on the provison that hosting costs are removed • Heatherlands- Approved • Riverside - Approved • Gladstone – Approved  Urgent care revised proposal - St Hilary GI  Urgent Care pilot Heatherlands MC.doc  Urgent Care pilot Riverside Surgery.do  Urgent Care proposal 2012 Gladst **3.3 Prescribing Support Coordinators.** The Chief Clinical Officer described the structure that practices currently have in place with regard to medicines management support, and how this structure has supported the practice in achieving QIPP indicators. The proposal submitted by Wirral Alliance is to appoint lower graded workers (e.g. technicians) to look at making savings on a day to day basis in relation to over prescribing and wastage of medicines. The Chief Officer clarified that the practices have agreed to the proposal in principle, but they may work this differently for their practice.  Practice Based Prescribing Support C The Approvals Committee approved the proposal.	**IS**
AC/12-13/20	**ITEMS FOR INFORMATION**	
	No items were discussed.	

REF NO.	MINUTES	ACTIONS
AC/12-13/21	**ANY OTHER BUSINESS**	
	Mike Roach enquired if an addition could be added to the template, which was cost savings to be made. This was agreed by the group with the caveat that not all proposals would be able to quantify the amount saved in the first instance. It was noted that there is not a meeting scheduled for December, however in accordance with the terms of reference, this could be arranged via the chair if required.	**MB**
AC/12-13/22	**DATE AND TIME OF NEXT MEETING**	
	The next meeting is Friday 18th January 2012 at 9.30am in Room 539 at Old Market House.	

RISK REGISTER - Master

Risk ID	Date	Source	Risk Description	Organisational Objectives (reference to detail)	Impact	Likelihood	Current Matrix Score	Previous Matrix Score	Trend	Driver for Change in Trend	Rationale	Key Control Established	Key Gaps in Control (reference to evidence)	Assurance on Controls (reference to evidence)	Gaps in Assurance (reference to evidence)	Action	Owner	Date of next review	Date of last review	Status
1	3.07.2012	Gov Body	Increase in activity for GP's as a result of the introduction of NHS111		3	3	9.00	9.00	–			Current provision of primary care / urgent care services - ability to absord additional activity	Unknown impact of 111 Service Impact	Monitoring of Primary Care/ urgent care activity and performace of NHS111 through information flows	Timely impact on monitoring of primary care activity	Monitor Information regarding implemention of 111	Governing Body	As further information becomes available	Feb-13	On-going
2	Ongoing	CSS	Reduction in local expertise and organisational memory due to PCT staff leaving		2	3	6.00	6.00	–			CSS / CCG Transitional Arrangements, Procedure Notes, CSS SLA, Legacy Documentation, Appropriate Handover	Individuals leaving before handover process is complete	CSS SLA Arrangements ensuring continuity, locality link involved in CSS Operational Group Meetings	SLA still in infancy	Continue development of SLA, transitional arrangements, clarity of responsibilities	Chief Officers	As further information becomes available	Feb-13	On-going
3	24.07.12 / 28.08.12 / 27.09.12	Gov Body / QPF / WHCC	Overperformance on WUTH Contract	Financial Management	4	5	20.00	20.00	–			Financial / Activity Reporting through QPF / Gov Body. Divisional Reporting / Practice Level Reviews - Action Plans	Ability to influence contract performance - Implementation of Action Plans	Regular Monitoring through committee / gov body structure, Use of Contigency Funds / Planned Slippage to offset	Ability to influence behaviour	Review performance areas, initiate action plan to address performance issues	Divisions	Mar-13	Feb-13	On-Going
4	28.08.12	QPF	Inability to monitor CT contract performance / outcome measures due to unavailability of information	Quality / Financial Management on Cost Per Case / Impact on Future Commissioning Intentions	2	4	8.00	8.00	–			CT Contract Monitoring / (Contract Query raised), Refinement of KPI's	Ability to influence provider behaviour	Regular Monitoring through contract monitoring process and subsequenty committee / gov body structure with ability to withold payment for non-provision of information as required	Ability to influence behaviour	Review contract query outcome, monitor action plan, Mersey Internal Audit Report - Data Quality Assurance Review	AC	Mar-13	Feb-13	On-Going
5	27.09.12	QPF	Contract Variation to Wirral NHS Community Trust Contract regarding implementation of NHS 111 to NHS Direct	Future Commissioning Arrangement regarding 111 service provision	3	5	15.00	10.00	↑			CT Contract Monitoring / (Contract Query raised), Part of NHS 111 Steering Group	Ability to influence implementation of NHS 111 Service, financial assumptions made with NHS 111 project	Urgent Care Meetings, Feedback from NHS 111 Workstream , Regular Monitoring through contract monitoring / negotiation process and subsequenty committee / gov body structure	Ability to influence implementation of NHS 111 Service	Continue workstream on progression of NHS 111 Service with NHS Direct and contract negotiations with Community Trust, Implementation Issues regarding model 1 / model2	AC	Mar-13	Feb-13	On-Going
6	27.09.12	QPF	Child Health Information System (CHIS) - Imminent Risk of Crashing	Provision of relevant Information System supporting appropriate statutory requirements	4	2	8.00	8.00	–			CT Contract Monitoring, CHIS Replacement Project via WHIS/ CICT	Lack of clarity regarding Responsible Officer / Availability of Project Plan	Regular Monitoring through committee / gov body structure, also raised via Public health Governance Group	Ability to prevent system failure	Project Plan in Place for CHIS system replacement (PARIS)	Rosemary Curtis ?	Mar-13	Feb-13	On-Going

7	24.10.12	WGPCC	WGPCC will fail to meet IAPT waiting time targets due to performance of one provider	Quality / Patient Access	2	5	10.00	10.00		Improved waiting times at last data submission		Action plan agreed with provider, including weekly submission of data and bi-weekly monitoring meetings	Provider dealing with old waiting list as well as new patients referred	Action plan dealing with both groups of patients will be monitored and reviewed by board on a monthly basis	Demand continues to rise for this service	Action plan agreed with Provider	Christine Campbell / Dr Oates	Mar-13	Feb-13	On-Going
8	31.10.12	QPF	Non-Compliance with Information Governance Standards by March 2013	Statutory Responsibility	4	2	8.00	8.00				IG Toolkit Assessment Work Programme to ensure compliance with required level by March 2013	Development of IG Policies / Procedures and implementation within CCG	Regular Monitoring through QPF and Audit Committee Meetings & Information Governance Manager work Programme through CSU SLA	Ensure Implementation of required standards	IG Toolkit Monitoring Programme	SIRO (CFO)	Mar-13	Feb-13	On-Going
9	06.11.12	Gov Body	Commissioned Out of Hospital Budgets, increase in package costs, Restitution Cases	Achieve Financial Balance	3	4	12.00	12.00				Financial / Activity Reporting through QPF / Gov Body. CSU SLA Monitoring Process	Time lag in information recieved, external stakeholders pursuing restitution cases	Regular Monitoring meetings with CSU, Top 10 package reviews, pro-active approach to new cases	Ability to influence behaviour	Review performance areas, initiate action plan to address performance issues	Governing Body	Mar-13	Feb-13	On-going
10	20.10.12	Gov Body	Impact of Local Authority Budgets Cuts	Financial Management / Service impact across Economy	3	5	15.00	15.00				Impact Assessment of Chief Executive Options Appraisal on NHS Budgets	Quantify Impact	Financial Planning and Budget Setting Process	Ability to manage impact of cuts	Action Plan for impact assessment	Governing Body	Mar-13	Feb-13	On-going
11	20.10.12 & 24.12.12	WGPCC	Risk of Consortium being unable to utilise its total allocation of efficiency resources due to slippage in several schemes becoming operational	Financial Management	2	0	0.00	0.00		WGPCC review of expenditure plans		Expenditure being monitored and support offered to practices around use of resources	Not all practices able to commit resources by deadline and WGPCC unable to commit resources to schemes before end of April	Plan being developed for alternative use of uncommitted resources before end of March 2013	WGPCC practices will need to agree proposals	Proposal taken to member practices for use of unutilised resources at practice member forum 5.12.12. New Investment Areas agree	Christine Campbell	Feb-13	Feb-13	Completed
12	06.12.12	WACC	Investment in agreed projects being concluded by end March 2013	Non-Recurring investment plans	1	0	0.00	6.00	↓			Weekly reviews of plans	Timescales for financial commitment to be made - by end February	Reviewed by WA Board on regular basis	Ability to implement investment schemes	Monitor Scheme slippage by CFO on monthly basis	Iain Stewart	Feb-13	Feb-13	Completed
13	06.12.12	WACC	CCG Constitution - refusal to sign agreement by some member practices	CCG Authorisation	3	3	9.00	9.00				Provision of up to -date information on progress of authorisation	Clarity on signed requirement for authorisation	Regular updates to Governing Body	Ability to influence behaviour	Identify key outstanding / unresolved issues	Dr Mark Green	Mar-13	Feb-13	On-going
14	06.12.12	WACC	Impact of NHS 111 on patient safety and demand shift to practices	Urgent Care Strategy	3	3	9.00	9.00				GP membership of QIPP Team to influence implementation	Centralised aspects of service that cannot be influenced	Regular updates to 111 Steering Group /QIPP Workstream & Governing Body	Ability to influence behaviour and implement robust service model	Continue workstream on progression of NHS 111 Service with NHS Direct and contract negotiations with Community Trust	Dr Bryan Conlan	Mar-13	Feb-13	On-going
15	06.12.12	WACC	Forecast overspend as at end March 2013	Financial duty to balance	1	3	3.00	6.00	↓			Demand management initiatives in place	Time-lag for initiatives impacting on outcomes	Reviewed by WA Board / QPF committee on regular basis	Increased Activity continues to rise / demand mgt schemes have little / no effect	Review over performance areas, initiate action plan to address performance issues	Iain Stewart	Mar-13	Feb-13	On-going
16	31.01.13	QPF	Lack of demand data/activity plans to forward plan future needs due to unavailbility of business intellegence	Quality / Financial Management on Cost Per Case / Impact on Future Commissioning Intentions	3	4	12.00	12.00				SLA meeting with CSU/ buisness Intellgence team	Ability to lead contract negotiations. Ability to provide accurate national returns	Regular monitroing through CSU/SLA meetings. Escalation to CSU MD. Monitoring through QPF committee	Abilty to influence behaviour. Ability to plan	Programme of work defined with CSU. Additional technical support in place	LQ/MB	Mar-13	Feb-13	On- going
17	31.01.13	QPF	Late reporting and undertaking of root cuase analysis following SI by CWP	Quality/ contracting issue	3	4	12.00	12.00				Quality Leads meeting/ CWP contract meeting/QPF	Ability to monitor provider performace	Regular montioring via CWP quality. CWW quality leads meeting	Ability to monitor a safe service is being delivered. Ability to assess if lessons have been learnt	Quality leads summit with provider. CCG quality committee	LQ	Mar-13	Feb-13	On-going
18	07.02.13	WACC	GP capacity to attend key meetings	GP Engagement / Redesign Agenda	2	3	6.00	0.00		New Item		Considering different model for clinical backfill	Time-lag to establishing model	Discussion at Alliance Board Meetings / Clinical Strategy group	Abilty to create capacity		Iain Stewart	Mar-13	Feb-13	On-going
19	13.02.13	WGPCC	Primary Care Mental health budget pressure due to overperformance and high DNA rate	Financial duty to balance	3	3	9.00	0.00		New Item		Regular contract monitoring meeting with provider, and with CCG finance and CSU contracting leads, to manage capacity and demand within available resources	Not a block contract so alternative means of managing demand within available resources need to be found	Working with contracting team to determine amendments that can be made to pathway in order to manage demand	Increase in demand and referrals	Review referral rates per practice; explore use of step 2 within contract with a view to reducing reliance upon the more advanced and	CC	Mar-13	Feb	Ongoing

Insert Rows Above This Line Only

Gov Body	Completed
WACC	On-going
WGPCC	Outstanding
WHCC	
PFQ	
G&A	
CSG	

Impact Values	
Negligible	1
Minor	2
Moderate	3
Major	4
Catastrophic	5

CSS

Probability Values	
Rare	1
Unlikely	2
Possible	3
Likely	4
Almost Certain	5

Green/Yellow/Red Threshold Values	
Green - maximum score	4
Yellow - minimum score	5
Yellow - maximum score	12
Red - minimum score	15