Checklist for the Review and Approval of Procedural Documents
To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

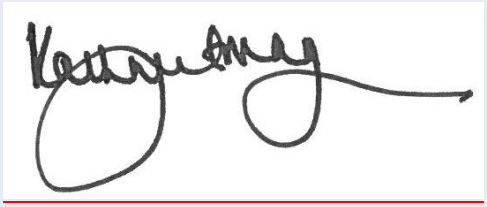
	Yes/No/ Unsure	**Comments**
Title of Document		Information Governance Framework
Could this policy be incorporated within an existing policy?	no	It's a requirement of the IG Toolkit
Does this policy follow the style and format of the agreed template?	yes	
Has the front sheet been completed?	yes	
Is there an appropriate review date?	yes	
Does the contents page reflect the body of the document?	yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	yes	Information Governance Toolkit Requirements
Are all appendices appropriate and/or applicable?	yes	
Have all appropriate stakeholders been consulted?	yes	

Has an Equality Impact Assessment been undertaken?	yes	
Is there a clear plan for implementation?	yes	
Has the document control sheet been completed?	yes	
Are key references cited and supporting documents referenced?	yes	
Does the document identify which Committee/Group will approve it?	yes	Executive Team
Plans for communicating policy to – staff; practice membership; public (as appropriate)	yes	Via the staff intranet and weekly staff news

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Caroline Hall	Date	08.01.18
Signature			

Committee Approval

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.

Name	Kathryn Magson	Date	08.01.18
Signature			

Herts Valleys CCG Information Governance Management Framework

Version Number	4.0
Accountable Director	Chief Finance Officer (Senior Information Risk Owner)
Responsible Post holder	Caroline Hall
Date Approved	8th January 2018 – Executive Team
Approved By	
Review Date	January 2019
Stakeholders engaged in development/review	Information Governance Group – approved 07/12/2018

Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to within the Information Governance Toolkit as the organisation's Information Governance Management Framework.

This framework should include detail of:

- Senior Roles
- Key Policies
- Key Governance Bodies
- Resources
- Governance Framework
- Training & Guidance
- Risk & Incident Management

Senior Roles

Chief Executive

The Chief Executive of the CCG and has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance, through the Statement of Internal Control that all risks to the CCG, including those relating to information, are effectively managed and mitigated**.**

Senior Information Risk Owner (SIRO)

The SIRO for Herts Valleys CCG is the Chief Finance Officer,

The SIRO will act as advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control in regard to information risk. The SIRO is expected to understand how the strategic business goals of the organisation may be impacted by information risks.

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk

Policy and associated risk management Strategy and processes. They will provide leadership and guidance to Information Asset Owners (IAO's)

The key responsibilities of the SIRO are to:

a) Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework

b) Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control

c) Review and agree action in respect of identified information risks

d) Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff

e) Provide a focal point for the resolution and/or discussion of information risk issues

f) Ensure the Board is adequately briefed on information risk issues

The SIRO will be supported in their role by the HVCCG and Bedfordshire CCG IG Team.

Information Asset Owner

The Information Asset Owners (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the CCG. It is a core IG objective that all Information Assets of the CCG are identified and that the business importance of those assets established.

The IAO is expected to understand the overall business goals of the CCG and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes
- How information is created, amended or added to over time

- Who has access to the information and why

Caldicott Guardian

The Caldicott Guardian for Herts Valleys CCG is the Director of Nursing and Quality

The Caldicott Guardian plays a key role in ensuring Herts Valleys CCG satisfies the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of the organisation, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Caldicott Function

In Herts Valleys CCG the Caldicott support function will be undertaken by the Bedfordshire and Herts Valleys CCG IG Team.

The key responsibilities of the Caldicott Function are to:

a) Support the Caldicott Guardian

b) Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented

c) Ensure compliance with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training

d) Complete the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment

e) Provide routine reports to senior management on Confidentiality and Data Protection issues

Data Protection Officer

Public authorities **must** appoint a data protection officer (DPO). The Head of IM&T is the DPO for HVCCG.

HVCCG DPO role includes:

- To inform and advise HVCCG its staff about their obligations to comply with the General Data Protection Regulation (GDPR) and other data protection laws.

- To monitor compliance with the GDPR and other data protection laws, including managing HVCCG internal data protection activities, advise on data protection impact assessments (PIA's); train staff and conduct internal audits.
- To be the first point of contact for individuals whose data is processed (employees, patients etc.).

Information Governance (IG) Manager (within HVCCG)

The IG Manager is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks, some of which will be delegated to the IG Team, include:

a) Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities

b) Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements

c) Providing direction in formulating, establishing and promoting IG policies

d) Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives

e) Ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported

f) Ensuring that the annual assessment and improvement plans are prepared for approval by the CCG Board in a timely manner.

g) Ensuring that the approach to information handling is communicated to all staff and made available to the public

h) Ensuring that appropriate IG training is made available to staff and completed as necessary to support their duties

i) Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards

j) Monitoring information handling activities to ensure compliance with law and guidance

k) Providing a focal point for the resolution and/or discussion of IG issues

l) Consider any breaches of Data Protection, Confidentiality and IT Security and take appropriate action

m) Act in advisory capacity to staff on Data Protection and Confidentiality in conjunction with the Caldicott Guardian

Key Policies

Herts Valleys CCG has the following policies and procedures in place to support the Information Governance agenda:

- Information Governance Policy
- Confidentiality & Data Protection Act Policy
- Information Sharing Policy
- Safe Haven Policy
- Information Security Policy
- Information Lifecycle Management Policy & Strategy
- Subject Access Request Policy & Procedure
- Information Risk Policy
- Business Continuity Strategy
- Freedom of Information Policy
- Environmental Information Regulations
- Incident Reporting Policy
- System Level Security Policies
- Network Security Policy
- Acceptable Use Policy
- Mobile Working Procedure
- Forensic Readiness Policy
- Privacy Impact Assessment Policy & Procedure

Any new/amended policies are notified to staff. All policies are also posted on the CCG's Intranet.

Key Governance Bodies

Information Governance Group

Senior Leaders Team

See Senior Leaders Team of Reference

Quality Committee

The responsibility of this group is to oversee the planning and delivery of Information Governance within the CCG. Their Terms of Reference in relation to information governance are:

a) To monitor progress against the Information Governance Action Plan, and provide assurance to the CCG Board on its progress.

b) To review the annual Information Governance assessment for sign off by the Board

CCG Board

The responsibilities of the CCG Board in relation to information governance are:

a) To ensure information governance is integrated into the broader governance of the organisation, and regarded as important as financial and clinical governance in organisational culture

b) To consider outcomes from annual internal audit of IG before sign off and inclusion in annual report

c) Board members to undertake face to face and online IG training on an annual basis

d) To review and sign off the annual Information Governance assessment

e) To ensure that all organisations from which care is commissioned, including the third sector, are brought within the NHS Information Governance Assurance Framework

Resources

Information Security Officer

The Information Security Officer (ISO) for the CCG is within the HBL ICT function. The ISO is tasked with providing advice on all aspects of information security and risk management, utilising their own expertise and, where necessary, external advice. The key responsibilities of the ISO are:

a) Draft and/or maintain the currency of the organisation's Information Security policy

b) Ensure security accreditation of information systems in line with the organisation's approved definitions of risk

c) Ensure compliance with the information security components of the IG toolkit, contributing to the annual IG assessment

d) Ensure all arrangements for managing information security are effective and aligned with the organisation's Information Security and Risk Policies

e) Provide regular information security risk assurance reports to the SIRO/IAO's via the Information Governance Steering Group

f) Co-ordinate the work of other staff with information security responsibilities

g) Co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach. Keeping the SIRO and IAO's informed of security incidents, impacts and causes, resulting actions and learning outcomes

h) Assist in the drafting of System Level Security Policies

i) Assist in the development of Business Continuity Management arrangements for key information assets

j) Advise in the development of a Network Security policy and controls for the secure operation of ICT networks, including remote/teleworking facilities

k) Provide advice and guidance regarding the implementation of controls to mitigate against malicious or unauthorised mobile code

l) Assist in designing and configuring access controls for key systems

m) Assist in developing the organisations Information Asset Register

n) Develop and document an action plan for the delivery of all specific activities involving the ISO

Freedom of Information Lead

. The main responsibilities of the HVCCG FOI Lead are:

a) Ensure the CCG complies with all aspects of the Act, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings, etc.

b) Provide reports to the Board highlighting resource, performance and compliance issues

c) Draft and/or maintain the currency of the organisation's FOI policy

d) Ensure that all staff are aware of their personal responsibilities for compliance with the Act and adhere to organisational policies and procedures

e) Ensure training and written procedures are widely disseminated and available to all staff

f) Ensure the general public has access to information about their rights under the Act

g) Establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times

h) Liaise and work with other functions responsible for information handling activities, for example Caldicott Guardian, data protection and information security staff

i) Contribute to or liaise with external FOI networks or groups to keep updated on 'round robin requests'

Clinical Governance Lead

The Clinical Governance Lead for the CCG is the. Director of Nursing and Quality

Governance Framework

Staff Contracts

All CCG staff contracts currently contain Information Governance related clauses within them (see Appendix A)

Non-NHS Third Party Contract Confidentiality Clause

Any non-NHS third party with whom the organisation contracts should include as a minimum a confidentiality clause. Herts Valleys CCG also requests all third party contractors to sign a declaration that they are registered with the Information Commissioner for Data Protection Purposes and that they encrypt all mobile devices to minimum standard required by the NHS. (See Appendix A)

They must also include the contract clauses as defined in the DPA 2018 (to be published early 2018).

Acute Trust Contract

The Trust uses the standard contract for Acute Trusts which includes clauses relating to Information Governance (See Appendix A). For 2017/18 Information Governance has also been included in Contract Monitoring (See Appendix B).

They must also include the contract clauses as defined in the DPA 2018

Information Assets and Asset Owners

During 2017/18 Information Asset Owners and Information Asset Administrators will attend face to face training sessions on their roles and responsibilities, this training will be delivered by the Herts Valleys IG Team

As part of the CCGs Pseudonymisation Project work will continue to be undertaken during 2017/18 to identify the information contained in the assets, the users of the information, the uses of the information and whether the information will require pseudonymisation for those uses.

Training & Guidance

Training

The CCG includes Information Governance as part of its mandatory training for all staff annually.

All new staff are required to complete the Introduction to Information Governance training module via the online IG Training Tool, when they first join the CCG unless they have completed appropriate IG Training within the last year and can evidence this.

The CCG also requires all existing staff to complete online IG Training annually, if they have previously completed the Introduction to Information Governance they can complete the Refresher Module.

The CCG has identified other modules of the IG Training Tool that those with roles relating to Information Governance will be required to undertake (see Appendix F). Those staff members involved will be informed of the additional modules that they are required to complete, these will be completed using the E Health Learning training Tool.

In addition to the above any member of staff involved in an Information Governance related incident may be required to undertake one or more modules of the IG Training Tool, the modules to be taken will depend on the type of incident and the outcomes of any investigations into the incident.

Guidance

The CCG currently uses the Confidentiality Code of Conduct tailored to individual staff groups/teams/department needs.

Further guidance for staff can be found in the CCGs Information Governance related policies as well as on the intranet

Incident Management

The CCG has an Incident Reporting Policy. All data breaches/near misses must be logged as an incident. An IG incident form must be completed for each incident/near miss. The Information Governance Manager will investigate and report each incident following the HSCIC guidance, All data breaches are reported to the Senior Leaders Team, any beaches

recorded as a potential or level 2 data breach, will be reported to the SIRO and Caldicott Guardian in the first instance.

For information and guidance on reporting an IG breach please contact the HVCCG IG team on 07825 852677

APPENDIX A

STAFF CONTRACT CLAUSES

- **Confidentiality**

During the course of your duties you are likely to come into contact with personal information about patients and or staff. You are required to keep all patient information confidential unless disclosure is expressly authorised by your employer. Misuse of or a failure to properly safeguard confidential data will be regarded as a disciplinary offence and may result in your dismissal. Under the Data Protection Act you and the organisation may be prosecuted for this or be liable for an action for civil damages. Personal information includes name, address, date of birth, gender, photographs or images, description of appearance or characteristic (this list is not exhaustive) Because health records are regarded as particularly sensitive and confidential information, they are also subject to Caldicott guidelines. These state that information should only be shared where there is a need to know in relation to the care of the patient. If in doubt about sharing information always check with the organisation Policies or your line manager.

You should read the NHS Code of Practice in relation to Confidentiality and ensure that you understand and comply with the guidance provided. If an unauthorised disclosure is made by you after you have left the organisation, the organisation may take legal action against you.

During the course of your duties you are likely to record information about individuals. It is important that this information is recorded as accurately as possible and in the appropriate place. This is a requirement of the Data Protection Act.

You may also, during the course of your employment, have access to commercially sensitive material and information, disclosure of which is prohibited. The organisation may take legal action against you should any information of this nature be disclosed or inappropriately used after you have left the organisation.

As a public body the organisation is required to provide information to the public under the Freedom of Information Act on request. Any documents which you produce including letters and e-mails may be subject to such a request and it is a criminal offence to destroy information in order to prevent a Freedom of Information request. You should ensure that you follow the organisation's Policy on the retention and disposal of records.

You must not, whether during your employment with the organisation, or after the end of it, whether you resign or are dismissed by the organisation, unless expressly authorised to do so, make any disclosure to any unauthorised person or use any confidential information relating to the business affairs of the organisation. This includes any detail about the organisation's clients and employees, actual, potential or past and all details relating to information on any of the organisation's databases ensuring that printouts are treated carefully.

APPENDIX B

CONFIDENTIALITY CLAUSES FOR NON-NHS 3RD PARTY CONTRACTS

1. The CONTRACTOR shall process information in accordance with the standards laid down in the Health & Social Care Information Governance Toolkit (IG). The CONTRACTOR will have in place an IG Management Framework incorporating as a minimum a Caldicott Guardian and Data Protection Lead and have full access to adequate technical information security expertise and support. The IG Management Framework will have implemented IG related policies and procedures covering the aspects of Data Protection, Confidentiality, information sharing, information security, records management and data quality. The CONTRACTOR shall be required to have the ability to pseudonymise patient information where the COMMISSIONER requests data for service planning and performance management and any other secondary uses. IG training will be provided to all the CONTRACTOR's employees on an annual basis. The CONTRACTOR shall support the COMMISSIONER by providing relevant information to enable the COMMISSIONER to meet its obligation under the Freedom of Information Act 2000.

2. The CONTRACTOR shall, in reference to the service defined in this AGREEMENT, ensure that personal information is handled appropriately with regards to all relevant legislation. This shall include the Common Law Duty of Confidence, Data Protection Act 1998 and Article 8.1 of the Human Rights Act concerning privacy, Computer Misuse and Freedom of Information Acts.

3. The CONTRACTOR shall submit an annual Connecting for Health Information Governance toolkit assessment and shall have achieved at least level 2 on all requirements or have submitted an action plan to do so, for approval by the COMMISSIONER.

4. Where the CONTRACTOR is processing personal data,

   a. the CONTRACTOR shall have a full and current registration with the Office of the Information Commissioner.

   b. the CONTRACTOR shall adhere to the Confidentiality NHS Code of Practice and Care Record Guarantee.

   c. the CONTRACTOR shall be an independent Data Controller.

   d. the CONTRACTOR shall inform patients about recording and use of patient information, why it is recorded and who it is disclosed to. Patients/clients shall have access to a privacy notice to support this process (formally known as a

fair processing notice). Verbal consent to share information with other organisations for the direct delivery of care shall be recorded in the patients' notes.

5. Person identifiable information (PII) shall not be shared for secondary uses (not for the direct delivery of healthcare) with other organisations, unless the CONTRACTOR has explicit patient consent, or the CONTRACTOR is required by law or if there is an overriding public interest. However, pseudononymised personal information may be shared for secondary uses.

6. The CONTRACTOR shall be responsible for establishing information sharing agreements with other third party organisations (including the COMMISSIONER), where the sharing of PII is necessary. The CONTRACTOR shall obtain an Information Sharing Agreement from the COMMISSIIONER for the purposes of establishing any agreements to share information.

7. The Contractor shall refer requests for access to health records, within 2 working days, to the COMMISSIONER's Head of Information Governance for processing.

8. The CONTRACTOR shall ensure that CONTRACTOR staff are provided with training about how handle PII appropriately in relation to the service provided. The CONTRACTOR shall also ensure that staff are reminded regularly of their responsibilities for safeguarding PII and that these requirements are set out in staff contracts of employment.

9. The CONTRACTOR shall ensure that CONTRACTOR policy and procedures regarding data protection and information security shall be readily accessible to all staff.

10. The CONTRACTOR shall ensure that policies, processes and procedures are established for timely, accurate and complete capture of PII related to the service, and its use. CONTRACTOR policies shall set out how checks on quality of data shall be undertaken.

11. The NHS number shall be used on all clinical records and correspondence in accordance with the corresponding patient safety notices.

12. The CONTRACTOR shall comply with the NHS Records Management Code of Practice, Schedule 2 with regards to appropriate retention and disposal requirements for the information/records collected as part of the service.

13. The CONTRACTOR shall dispose of all IT equipment in a secure manner, which ensures that any data held on that IT equipment is completely inaccessible, even by using specialist technical recovery techniques.

14. The CONTRACTOR shall ensure that all records are stored in locations which are only accessible to authorised individuals. All electronic data shall be stored on secure servers.

15. The CONTRACTOR shall ensure that all information systems feature appropriate access controls which allow access to the system, and the information stored therein only by authorised individuals who have a reasonable justification to access stored information.

16. The CONTRACTOR shall monitor the effectiveness of the controls it has in place to protect confidentiality. The CONTRACTOR shall ensure that any potential or actual breaches of practice by staff are identified, reported to the Commissioner, investigated promptly and that action is taken to address weaknesses, in accordance with documented information security event procedures. The COMMISSIONER shall be entitled to send a representative to audit the policies and processes in place.

17. The CONTRACTOR shall ensure that records and systems are not at unnecessary risk from environmental hazards such as fire, theft, flood. The CONTRACTOR shall ensure that back-up copies of records are made and that such back-up copies are stored securely at an alternate safe location.

18. The CONTRACTOR shall ensure that records of systems are not at unnecessary risk from loss of power, corruption of data or avoidable technical failure. The CONTRACTOR shall maintain Business Continuity Plans and shall ensure that such plans are tested regularly.

19. The CONTRACTOR shall ensure that data is encrypted fully to current Commissioner and Connecting for Health standards before such data is transferred electronically including by mobile devices.

20. Personal data shall not be transferred overseas without the express permission of the COMMISSIONER, and only under strict conditions to be determined.

21. The CONTRACTOR shall ensure that appropriate safeguards against loss are in place to protect PII being transported via any form of physical media. The CONTRACTOR shall adopt Safe Haven principles and procedures.

22. The CONTRACTOR shall forward within 2 working days of receipt any Freedom of Information requests to the COMISSIONER Information Governance Lead for processing. OI requests received to the Commissioning IG Team for processing within 2 working days.

23. The CONTRACTOR shall keep all records pertaining to services commissioned in accordance with section 46 of the Freedom of Information Act, to facilitate efficient retrieval of information.

24. The CONTRACTOR shall agree to indemnify and keep indemnified the COMMISSIONER and any beneficiary against all claims and proceedings and all liability, loss, costs and expenses incurred in connection therewith by the COMMISSIONER and any beneficiary as a result of any claim made by any individual or other legal person in respect of any loss, damage or distress caused to that individual or other legal person as a result of the CONTRACTOR's unauthorised processing or unlawful processing, destruction of and/or damage to any personal data processed by the CONTRACTOR, its employees or agents in the CONTRACTORs performance of the contract or as otherwise agreed between the parties.

APPENDIX C

ACUTE, COMMUNITY, AMBULANCE TRUST CONTRACT CLAUSES

60. DATA PROTECTION, FREEDOM OF INFORMATION AND TRANSPARENCY

60.1 The Parties acknowledge their respective duties under the DPA and FOIA and shall give all reasonable assistance to each other where appropriate or necessary to comply with such duties.

Data Protection

60.2 The Provider shall achieve a minimum of level 2 compliance against all requirements in the relevant NHS information governance toolkit applicable to it. Where the Provider has not achieved level 2 compliance by the Service Commencement Date, the Co-ordinating Commissioner may, in its sole discretion, agree a plan with the Provider to enable the Provider to achieve level 2 compliance e within a reasonable time.

60.3 To the extent that the Provider is acting as a Data Processor on behalf of a Commissioner, the Provider shall, in particular, but without limitation:

60.3.1 only process such Personal Data as is necessary to perform its obligations under this Agreement, and only in accordance with any instruction given by the Commissioner under this Agreement;

60.3.2 put in place appropriate technical and organisational measures against any unauthorised or unlawful processing of such Personal Data, and against the accidental loss or destruction of or damage to such Personal Data having regard to the specific requirements in Clause 60.4.3 below, the state of technical development and the level of harm that may be suffered by a Data Subject whose Personal Data is affected by such unauthorised or unlawful processing or by its loss, damage or destruction;

60.3.3 take reasonable steps to ensure the reliability of Staff who will have access to such Personal Data, and ensure that such Staff are aware of and trained in the policies and procedures identified in Clauses 60.4.4m 60.4.5 and 60.4.6 below; and

60.3.4 not cause or allow such Personal Data to be transferred outside the European Economic Area without the prior consent of the relevant Commissioner.

60.4 The Provider and each Commissioner shall ensure that Personal Data is safeguarded at all times in accordance with the Law, which shall include without limitation obligations to:

60.4.1 perform an annual information governance self-assessment using the NHS information governance toolkit;

60.4.2 have an information governance lead able to communicate with the Provider's board, who will take the lead for information governance and from whom the Provider's board shall receive regular reports on information governance matters including, but not limited to, details of all incidents of data loss and breach of confidence;

60.4.3 (where transferred electronically) only transfer data (i) where this is essential having regard to the purpose for which the transfer is conducted; and (ii) that is encrypted to the higher of the international data encryption standards for healthcare and the National Standards (this includes, but is not limited to, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes);

60.4.4 have policies which are rigorously applied that describe individual personal responsibilities for handling Personal Data;

60.4.4A report all incidents of data loss and breach of confidence in accordance with department of health and or NHS CB and/or HSCIC guidelines;

60.4.5 have a policy that allows it to perform its obligations under the NHS Care Records Guarantee;

60.4.6 have agreed protocols for sharing Personal Data with other NHS organisations and (where appropriate) with non-NHS organisations; and

60.4.7 where appropriate have a system in place and a policy for the recording of any telephone calls in relation to the Services, including the retention and disposal of such recordings.

Freedom of Information and Transparency

60.5 Where the Provider is not a Public Authority, the Provider acknowledges that the Commissioners are subject to the requirements of the FOIA and shall assist and co-operate with each Commissioner to enable the Commissioner to comply with its disclosure obligations under the FOIA. Accordingly the Provider agrees:

60.5.1 that this Agreement and any other recorded information held by the Provider on the Commissioners' behalf for the purposes of this Agreement are subject to the obligations and commitments of the Commissioners under the FOIA;

60.5.2 that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under the FOIA is a decision solely for the Commissioner to whom the request is addressed;

60.5.3 to assist the Commissioners in responding to a request for information, by processing information or environmental information (as the same are defined in the FOIA) in accordance with a records management system that complies

with all applicable records management recommendations and codes of conduct issued under section 46 of the FOIA, and providing copies of all information requested by a Commissioner within 5 Operational Days of such request and without charge.

60.6 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Agreement is not Confidential Information.

60.7 Notwithstanding any other term of this Agreement, the Provider hereby consents to the publication of this Agreement in its entirety including from time to time agreed changes to the Agreement subject to the redaction of information that is exempt from disclosure in accordance with the provisions of the FOIA.

60.8 in preparing a copy of this Agreement for publication pursuant to Clause 60.7 the Commissioners may consult with the Provider to inform decision making regarding any redactions by the final decision in relation to the redaction of information shall be at the Commissioners' absolute discretion

60.9 The Provider shall assist and cooperate with the Commissioners to enable the Commissioners to publish this Agreement.

APPENDIX D

ACUTE, COMMUNITY TRUST CONTRACT MONITORING

(1) Status of Information Governance Toolkit Assessment (i.e. started, completed, submitted) as at: 31st July, 31st October & 31st March

(2) For 31st July and 31st October: current %age score and anticipated year end %age score

(3) Prior to 31st March: current %age score split into 5 key areas (IG Management, Confidentiality & Data Protection Assurance, Information Security Assurance, Clinical Information Assurance, Secondary Use Assurance, Corporate Information Assurance)

In addition to the above the provider is to alert the CCG if at any time it does not meet the required attainment levels for the key (Statement of Compliance) criteria or will not be able to meet required timescales for submissions.

APPENDIX E

CALDICOTT FUNCTION SPECIFICATION AND IMPLEMENTATION PLAN

In accordance with the Information Governance Toolkit requirements the Caldicott function has been established since the inception of the Herts Valleys CCG. The Caldicott Guardian is required to be at Director Level and have a clinical background. The CCG's should also appoint a deputy Caldicott Guardian, also with clinical expertise, who will act on behalf of the main post holder in their absence.

The Caldicott Guardians will perform the functions as laid down in the Caldicott Guardian Manual, available on the Health & Social Care Information Centre website, and will be responsible for protecting patient and service user confidentiality and enabling information sharing. The Caldicott Guardian will also have a strategic role in representing and championing Information Governance requirements and issues at Board level. The role of the Caldicott Guardians will be specified and promoted throughout the IG Management Framework documentation and will be made readily accessible to staff via the CCG's staff intranet. This role will be primarily supported by the NHS Code of Confidentiality.

The Caldicott Guardians will be supported by the Bedfordshire IG team on issues concerning data protection. The IG Manager will manage the processing of requests for access to health records, (HVCCG does not hold any medical records in relation to treatment and care), the Caldicott Guardians will provide advice on the release of information to the Police and other agencies as appropriate.

The IG Manager will negotiate and develop information sharing agreements on behalf of the Caldicott Guardians, which will be reviewed by the IG Steering Group and signed by the Caldicott Guardian.

Where CCG staff feel that meeting IG standards may cause operational difficulties or they feel that meeting IG standards would compromise patient care or safety, they can apply to the Caldicott Guardian for a decision on whether an acceptable risk status can be agreed.

Incidents and issues relating to patient confidentiality will be reported to the Caldicott Guardian promptly and recorded and monitored in the Caldicott log which will be reviewed by the IG Steering Group. The IG Manager will ensure that the CCGs benefit from lessons learned by sharing at IG Steering Group meetings and, where relevant, within CCG Quality and Governance (or equivalent) Committees. The agreed acceptable risks will also be recorded in the Caldicott Log.

APPENDIX F

Information Governance Training Tool Modules

Data Security Awareness	All Staff
Caldicott Guardian in the NHS & Social Care	Caldicott Guardian
NHS Information risk Management for SIRO's & IAO's	SIRO, IAOs, ISO, All IG Staff
NHS Information Risk Management (Introduction)	ISO, All IG Staff
NHS Information Risk Management (Foundation)	ISO, All IG Staff
Information Security Guidelines	ISO, IG Manager
Access to Health Records	Any staff members who have responsibility for responding to Access to Health Records requests
Records Management & the NHS Code of Practice	Any staff members who have responsibility for Records Management
Records Management in the NHS	Any staff members who have responsibility for Records Management

Information Governance Training (Face to Face)

Information Governance for Board Members	All Board Members
Information Risk Management and Information Risk Assessment	SIRO, IAOs and IAAs

APPENDIX G

Herts Valleys CCG procedure for handling information related incidents

See HSCIC Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Please contact the HVCCG IG team on 07825 852677 for further information. Or Ruth.Boughton@HertsValleysCCG.nhs.uk