NHS
Herts Valleys
Clinical Commissioning Group

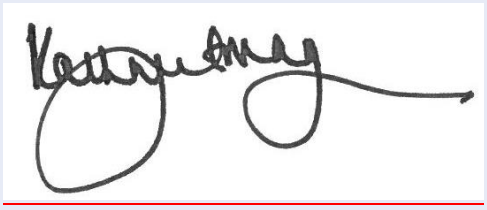
Checklist for the Review and Approval of Procedural Documents

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		HVCCG A Guide for Staff
Could this policy be incorporated within an existing policy?	No	
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?	No	Information Governance Staff Guidance
Are all appendices appropriate and/or applicable?	Yes	
Have all appropriate stakeholders been consulted?	Yes	
Has an Equality Impact Assessment been undertaken?	N/A	
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	Will be published on the staff intranet

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

A Guide for Staff

Version Number	2.0
Reviewed By	Ruth Boughton
Date Reviewed	November 2017
Approved By	Executive Team
Date Approved	January 2018
Name of Originator/Author	Ruth Boughton IG Manager
Responsible Director	Chief Finance Officer
Staff Audience	All staff
Date Issued	January 2018
Next Review Date	January 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
1.0		New document	29 January 2016	Head of Information Governance
			June 2016	IG Manager
2.0		Annual Review Data Protection Officer Role added Minor updates Approved by SIRO, Caldicott Guardian and Data Protection Officer	Nov 17 05/12/17	IG Manager

CONTENTS

Introduction

Information Governance (IG) is the practice used by all organisations to ensure that information is effectively managed and that appropriate polices, system processes and effective management accountability provides a robust governance framework for safeguarding information.

Information Governance enables organisations to embed policies and processes to ensure that personal and sensitive information is:

- Held securely and confidentially;
- Obtained fairly and efficiently;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared appropriately and lawfully.

NHS organisations hold numerous amounts of personal and sensitive information and all staff should be able to provide assurance that the Information Governance standards are incorporated within their working practices.

Personal and sensitive information can be contained within a variety of documents. For example:

- Health records;
- Staff information;
- Corporate information;
- Commissioning information;

It is important for staff to be aware of what constitutes personal and sensitive information. Further details on types of information are available within the Confidentiality module on the HSCIC – Information Governance Training Tool.

Legislation and Regulations

Members of staff should also be aware of the legislation surrounding Information Governance that stipulate how organisations should safeguard information, what processes are in place to use, secure and transfer information and also how patients

and members of public have access to personal/business information. The organisation must comply with the following:

- Data Protection Act 1998 (to be superseded by DPA 2018)
- Caldicott principles
- Freedom of Information Act 2000
- Privacy and Electronic Communications
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015 – Duty to Share

The CCG IG Team:

Trudi Mount, Head of IM&T Trudi.mount@hertsvalleysccg.nhs.uk

Ruth Boughton, HVCCG IG Manager Ruth.Boughton@Hertsvalleysccg.nhs.uk
Mobile 07825 852677

HVCCG FAQ

Information Governance Structure

Clinical Commissioning Group Chief Executive

The CCG Chief Executive has overall responsibility for Information Governance within the organisation. As Chief Executive they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Chief Executive is required to sign annually.

Clinical Commissioning Group Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for the CCG is the Chief Finance Officer with allocated lead responsibility for the organisation's risks and provides the focus for management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The IG Manager will support the SIRO in fulfilling their role.

Caldicott Guardian

The Caldicott Guardian is the Director of Nursing and Quality within the CCG with overall responsibility for protecting the confidentiality of person identifiable data (PID) and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to feedback any information governance issues to the CCG Board. The IG Lead will support the Caldicott Guardian in fulfilling this role.

The Information Governance Manager

The HVCCG IG Manager in conjunction with the Head of Information Governance Bedfordshire CCG IG team are responsible for ensuring the information governance programme is implemented throughout the CCG. The IG Manager is also responsible for the completion and annual submission of the Information Governance toolkit requirements for the CCG. The IG Manager will liaise with the Head of Patient Safety in relation to reporting, investigating and monitoring Serious Incidents Requiring Investigation (SIRI's) in relation to the requirements set out by HSCIC. Support the FOI lead to interpret and apply both the FOI and EIR Acts and. offer advice to and ensures the organisation complies with legislation, policies and protocols.

Data Protection Officer (DPO)

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 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 Asset Owners (IAOs)

The SIRO is supported by the IAOs. The role of IAO is to understand what information is held, what is added and what is removed, who has access to and why in their area. As a result, they are able to understand and address risks to the information assets they "own" and to provide assurance to the SIRO on the security and use of the assets. The IG Lead will support the IAOs in fulfilling their role.

Information Governance Toolkit

The IG toolkit is an Information Governance Assessment tool to measure the organisation's compliance. This is an annual return and has 28 requirements to fulfil and gather evidence.

The final assessment must be submitted by 31 March each year and is shared with the Care Quality Commission, Audit Commission and NHS England.

The CCG is required to achieve level 2 performance against all requirements identified in the information governance toolkit. Organisations must sign to provide

assurance they are meeting these requirements and must have robust improvement plans to address any shortfalls against other requirements.

Information Governance Mandatory Training

Every individual who works for the organisation is required to complete mandatory annual information governance training. This includes all new starters, existing and temporary members of staff and contractors. The CCG has a responsibility to ensure those working with our information are aware of the IG principles and the risks to the reputation of our CCG which may occur if processes are not followed.

All staff are required to complete training through the E Health Learning Tool.

The IG team have conducted a training needs analysis and identified IG training which will need to be completed by those within different job roles and functions.

All new starters, temporary staff and contractors working will need to complete the Introduction to Information Governance module. Existing staff who have already completed the Introduction to Information Governance module should then complete the Refresher module for subsequent years. However, existing staff can complete the introductory modules should they need more in-depth information governance training.

Caldicott Principles and Data Protection Act

The Caldicott Principles

The Caldicott Committee made recommendations aimed at improving the way the NHS uses and protects confidential information. All NHS employees must be aware of the seven Caldicott principles which apply to both patient and personal data.

Principle 1 – Justify the purpose – Why is the information needed?

Principle 2 – Don't use patient identifiable information unless absolutely necessary – Can the task be carried out without identifiable information?

Principle 3 – Use the minimum necessary patient identifiable information – Can the task be carried out with less information?

Principle 4 – Access to patient identifiable information should be restricted to required/relevant personnel

Principle 5 – Everyone with access to patient identifiable information should be aware of their responsibilities – lack of knowledge is not acceptable

Principle 6 – Understand and comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Confidentiality

Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This guide sets out the key principles and main "do's" and don'ts" that everyone should follow to achieve this for both electronic and paper records.

The common law of duty of confidentiality protects from disclosure information (whether personal or not) that "is given in circumstances giving rise to an obligation of confidence on the part of the person to whom the information has been given". This means that where information is passed in circumstances where a confidential relationship has been established, the person receiving the information is under a duty not to pass on the information to a third party. The duty is not absolute and information can be shared without breaching the common law duty if:

- The information is not confidential in nature; or
- The person to whom the duty is owed has given explicit consent; or
- There is an overriding public interest in disclosure; or
- Sharing is required by a court order or other legal obligation

When considering disclosure, a judgement must be made as to where the public interest lies (the more sensitive and damaging the information, the stronger the public interest in disclosure will need to be).

Information Sharing

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The CCG needs to ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

Staff sharing personal information with other agencies should be aware of the requirement to have an Information Sharing Agreement in place for the routine sharing of person identifiable data.

The IG team should be contacted for further advice regarding the development of information sharing agreements.

Consent

There are two different types of consent (this will change when the new DPA comes into force in May 2018).

Implied – is when consent is implied by the behaviour of the individual and specific written consent is not required. You must be sure that the individual is fully informed and aware that you will be sharing the information. An example of implied consent is if a GP tells a patient they will be referred to a specialist, unless the patient specifically requests that they do not want their information passed on, it can be shared with that specialist.

Explicit – is when fully informed consent must be obtained; this will usually be in writing. For example, a patient's details and medical records are requested by a research company, the patient would have to sign to give consent for their details to be released to the research company.

Whenever you share information make sure the individual to whom it relates is fully informed about what their information will be used for, who it will be shared with and how long it will be kept for.

For more information on sharing information and consent please contact the IG team.

Data Protection Act 1998 (until May 2018)

This Act regulates the processing of personal and or sensitive information for any living individual. This covers both electronic and paper records. It applies to personal information generally and not just health records.

Personal and sensitive information is data relating to any living individual that enables him or her to be identified either from that data alone or from that data in conjunction with other information. It therefore includes such items as name, address, age, race, religion, gender and information relating to physical, mental or sexual health.

The Data Protection Act mainly relates to how we process information. Processing means everything that is done with that information, for example, creating it, obtaining it, holding it, recording it, using it, sharing it and disposing of it.

Information Commissioner's Office

The role of the ICO is to uphold information rights in the public interest.

The ICO holds the Register of Data Controllers, handles concerns regarding data protection and takes action against people and organisation that breach the Data Protection Act 1998.

Subject Access Requests

Under the Data Protection Act 1998 all living individuals are “Data Subjects” and have a right to be informed of the following:

- If the CCG holds, stores or processes personal data about them;
- A description of the personal data held, the purpose for which it is processed and to whom the personal data may be disclosed;
- A copy of any information held; providing that it will not be deemed detrimental to their physical or mental health to receive the data that any third party data can be removed or redacted from the information or an exemption applies i.e. crime and taxation.
- To be informed as to the source of the data held.

Your personal information can only be obtained through the Subject Access Request Process. Please also refer to the ICO code of practice for further guidance.

Information Security

Within any organisation there will always be information risk. It is important those risks are identified, where possible minimised and managed. It is impossible to eliminate all risks.

The Senior Information Risk Owner (SIRO) owns the risk within the organisation and provides assurance to the Accountable Officer.

The SIRO is an Executive Board member who is familiar with information risks and provides the focus for the management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the CCG and for any services contracted for by the organisation.

Safe Haven

What is a safe haven?

A safe haven is a process by which sensitive and person identifiable information must be handled. A safe haven is needed to ensure the privacy and confidentiality of information and to meet legal requirements and the Department of health guidelines.

All sensitive and person identifiable information received by or sent from the CCG must be handled in accordance with the CCG’s Safe Haven Policy.

Safe Haven Fax Machines

The CCG’s fax machine is part of the Multi-Function Devices located within Hemel One.

Reporting breaches of security or confidentiality

The Information Commissioner's Office is able to issue monetary penalties to any organisation found to be in breach of the Data Protection Act. A fine of up to £500,000 may be incurred for a serious breach. The ICO can also conduct an investigation into less serious breaches which can lead to an organisation have an enforcement notice imposed upon them.

Each member of staff has a responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way.

If you require advice on reporting a near miss or a security breach via datix please contact the IG team or refer to the Incident Reporting Policy. .

Records Management

Records management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type from their creation all the way through to their lifecycle to their eventual disposal. The NHS has two categories of records, Health and Corporate.

Records can be held in paper (manual) or electronic form.

The NHS Records Management guidance gives advice on retention periods for both types of records; if in doubt please contact the IG team.