CCGs working together

Airedale, Wharfedale and Craven CCG
Bradford City CCG
Bradford Districts CCG

INFORMATION GOVERNANCE POLICY AND FRAMEWORK

Policy approved by: Audit and Governance Committees

Date: 9th October 2017

Next Review Date: September 2018

Version: 4.0

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Officer
Author:	Senior IG Specialist, eMBED
Date Approved:	9th October 2017
Committee:	Audit and Governance Committees
Version:	4.0
Review Date:	September 2018

Version History

Version no.	Date	Author	Description	Circulation
1.0	31 August 2014	IG Specialist, YHCS	Initial Draft	
2.0	31 August 2015	IG Specialist, YHCS	Reviewed and updated	
3.0	02 September 2016	Senior IG Specialist, eMBED Health Consortium	Reviewed and updated	
3.1	18 August 2017	Senior IG Specialist, eMBED Health Consortium	Reviewed and updated: • combined 3CCGs Policy • reference to GDPR • addition of DPO role • Addition of definition of data controller and data processor	Head of Governance (initial drafts), A&G Comms (final)
4.0	October 2017	Senior IG Specialist, eMBED Health Consortium	Approved by Audit and Governance Committees 9th October 2017	

Contents

INFORMATION GOVERNANCE POLICY AND FRAMEWORK

1. INTRODUCTION

1.1 NHS Airedale, Wharfedale and Craven Clinical Commissioning Group, Bradford City Clinical Commissioning Group and Bradford Districts Clinical Commissioning Group (hereafter known as the CCGs) recognise the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCGs also recognise the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which they process, store, share and dispose of information.

1.2 The Information Governance Policy and Framework sets out the CCGs' overall approach to the management of information governance and should be read in conjunction with the Information Governance Strategy and Strategic Vision and the other information governance policies and procedures.

2. AIMS

2.1 The aim of this policy is to ensure that all staff understand their obligations with regard to any information which they come into contact with in the course of their work and to provide assurance to the Governing Body that such information is dealt with legally, securely, efficiently and effectively.

2.2 The CCGs will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the Data Protection Act, the General Data Protection Regulation (GDPR) which will be in force as of the 25th May 2018, Records Management Guidance, Information Security Guidance and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit (IGT). These standards are:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

2.3 This policy supports the CCGs in their role as commissioners of health services and will assist in the safe sharing of information with their partners and agencies.

3 SCOPE

3.1 This policy must be followed by all staff who work for, or on behalf of the CCGs including those on temporary or honorary contracts, secondments, volunteers, pool staff, board members, Governing Body, Clinical Board, / Clinical Executive Members, students and commissioning support staff working for and behalf of the CCGs. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

3.2 This policy and framework covers:

All aspects of information within the organisation, including (but not limited to):

- Patient/client/service user information
- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by, or on behalf of, the organisation
- CCG information held on paper, floppy disc, CD, USB/memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transmission of information – verbal, fax, e-mail, post, text and telephone
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

3.2 Information governance within an independent contractor's premises is the responsibility of the owner/partners. However, the CCGs are committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

3.3 The CCGs recognise the changes introduced to information management as a result of the Health and Social Care Act 2012 and work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

3.4 Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY

4.1 Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy.

4.2 Audit and Governance Committees

The Audit and Governance Committees are responsible for the review and approval of this policy, related work plans and procedures and will receive regular updates on compliance and any related issues or risks.

The Audit and Governance Committees Terms of Reference (TOR) define the committee's roles and responsibilities which are delegated to them by the Governing Body.

4.3 Accountable Officer

The Chief Officer is the Accountable Officer of the CCG and has overall accountability and responsibility for information governance and is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to confidentiality and data protection, are effectively managed and mitigated.

4.4 Senior Information Risk Owner

The Chief Finance Officer is the Senior Information Risk Owner (SIRO) and has organisational responsibility for all aspects of risk associated with information governance, including those relating to confidentiality and data protection.

4.5 Data Protection Officer

Article 37(5) of the GDPR allows the role of DPO to be assigned to either a member of staff or to an external contractor, designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. These are:

- to inform and advise the organisation and its employees 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 assigning responsibilities, managing internal data protection

activities, advise on data protection impact assessments; train staff and conduct internal audits.

- To cooperate with the supervisory authority (the ICO in the UK);
- To act as the contact point for the supervisory authority and for individuals whose data is processed (employees, patients etc.).

Under GDPR, the role of DPO is protected and the organisation must ensure that:

- The DPO reports to the highest management level of the organisation – ie Governing Body level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

4.6 Caldicott Guardian

The Caldicott Guardian for the CCGs is Director of Quality. The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information.

4.7 Information governance lead

The senior level information governance (IG) lead for the CCGs, is the Associate Director of Corporate Affairs (supported by the Head of Governance). The IG lead is responsible for ensuring effective management, accountability, compliance and assurance for all aspects of IG and for liaising with the information governance team from Embed Health Consortium who provide agreed support to the CCGs.

4.8 Information asset owners and administrators

Information asset owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they are responsible for and that any changes introduced to their business processes and systems undergo a data privacy impact assessment (DPIA).

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

4.9 Heads of service/directors

Heads of service/directors are responsible for ensuring that they and their staff are familiar with this policy and its associated guidance. They must ensure that any breaches of the policy are reported, investigated and acted upon.

4.10 Employees

Information governance compliance is an obligation for all staff. Staff should note that there is a Non-Disclosure of Confidential Information clause in their contract and that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer system is a disciplinary offence, which could result in dismissal or termination of your employment contract, and must be reported to the SIRO and (in the case of health or social care records) the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to data protection and confidentiality. Under GDPR individuals can personally be fined and/or prosecuted where a data breach is deemed intentional or malicious.

4.11 Embed Health Consortium

The CCGs contract with Embed Health Consortium for Information Governance support and they can be contacted via the CCG IG Lead or emailing eMBED.infogov@nhs.net for advice.

4.12 Third Party Contracts

The CCGs will ensure that contracts with third parties providing services to, and on behalf of the CCGs, include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that contractors are aware of their IG obligations.

Clinical services

All clinical services commissioned by or on behalf of the CCGs will be required to ensure that:

- A suitable contract is in place to form a joint data controller relationship regarding the information required to effectively monitor commissioned services
- The services commissioned meet the requirements of the Data Protection Act and GDPR when providing services including, but not limited to, fair processing and until 25th May 2018, maintaining a registration with the Information Commissioner's Office, after which registration is no longer required.

- Completion of the annual Information Governance Toolkit and if requested, undertake an independent audit, to be disclosed to the CCGs in order to provide further assurance they have met expected requirements.

- Ensure privacy notices make individuals aware of the CCGs role in commissioning and the personal and sensitive data it may receive to undertake such a role.

- Ensure that where any IG incidents occur that they are reported to the CCGs via routes determined within the contract.

- Expectations regarding requests for information made under the Freedom of Information Act are set out.

- Ensure inclusions regarding exit plans are addressed following transfer of services or decommission of service e.g. Passing on data / deletion/ retention of data at end of the contract.

Support services

All support services that process information on behalf of the CCGs will be required to ensure that:

- A suitable contract/SLA is in place to form a data controller to data processor relationship where personal or personal sensitive data is managed on behalf of the CCGs

- The services commissioned meet the requirements of the Data Protection Act and GDPR including, but not limited to, fair processing and until 25th May 2018, maintaining a registration with the Information Commissioner's Office.

- Completion of the annual Information Governance Toolkit (if applicable) and at the request of the CCGs undertakes a compliance check/ audit, in order to provide assurance they have met expected requirements.

- That any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity.

- Report any known incidents or risks in relation to the use or management of information owned by the CCGs without delay.

- Expectations regarding providing information in relation to requests for information made under the Freedom of Information Act are set out.

- Ensure inclusions regarding exit plans are addressed following transfer of services or decommissioning of service e.g. passing on data / deletion/ retention of data at end of the contract.

5. DEFINITION OF TERMS

5.1 Personal Confidential Data

Personal Confidential Data (PCD) refers to all items of information in any format from which an individual might be identified or which could be combined with other available information to identify an individual and is information which has a duty of confidence. This includes (but is not limited to):

- Name
- Date of birth
- Post code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or hospital/practice number
- Date of death

5.2 Sensitive Personal Data

Certain categories of information are classified as sensitive personal data and additional safeguards are necessary when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Physical and mental health
- Genetic data (from 25th May 2018)
- Biometric data (from 25th May 2018)
- Social care
- Ethnicity and race
- Sexuality
- Trade union membership
- Political affiliations
- Religion
- Records relating to criminal charges and offences

5.3 Direct and Indirect care

The Caldicott Report (1997) defined direct and indirect care as follows:

Direct care

"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse

incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care"

Indirect care

Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment and financial audit.

The CCGs adhere to national guidance in relation to using Personal Confidential Data for commissioning purposes and recognise that such data can only flow where a clear legal basis enables this.

5.4 Consent

The processing of identifiable data is normally subject to gaining the freely given fully informed consent of the data subject, unless another legal basis is identified which permits such processing. An overview of these considerations is provided within the CCG Privacy Notice, available from the organisations websites.

For the CCGs to be compliant with the Data Protection Act, and the General Data Protection Regulation (from 25th May 2018) they must demonstrate consideration of all the Data Protection principles, the first of which states that processing must be fair and lawful. This means that patients need to be made aware of how their data is being used and that such processing takes place based on freely given fully informed consent.

If data is being used for direct care this consent may be 'implied' – i.e. the patient is advised of how the data will be used and can object/withdraw consent if they are not satisfied. For implicit consent to be effective, organisations must ensure patients are fully informed. Where data is being shared outside of direct care, 'explicit' (recordable) consent should be sought to ensure that patients are content with this.

5.5 Corporate information

Corporate information includes:

- Governing Body and meeting papers and minutes
- Tendering and contracting information
- Financial and statistical information
- Project and planning information

Corporate information could be accessible through the Freedom of Information Act either from the CCGs responding to a request for information or through

making information accessible via the CCGs' Freedom of Information Publication Schemes. Where any corporate information has a duty of confidence attached to it, the information may be exempt from release. Additionally, other exemptions of the Act could restrict release of certain corporate information.

5.6 Data Controller

'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

5.7 Data Processor

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

6. KEY PRINCIPLES AND PROCEDURES

6.1 Openness and transparency

- The CCGs recognise the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott, legislation and guidance.
- Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCGs will establish and maintain a Publication Scheme in line with legislation and guidance from the Information Commissioner.
- There will be clear procedures and arrangements for handling queries from patients, staff, other agencies and the public concerning personal and organisational information.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

- Legislation, national and local guidelines will be followed.

- The CCGs will undertake annual assessments and audits (through the IGT) of their policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under the Data Protection Act and GDPR using the CCGs Access to Records Procedure.
- The CCGs will have clear procedures and arrangements for liaison with the press and broadcasting media.

6.2 Legal compliance

- The CCGs regard all personal information as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.
- The CCGs regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCGs will establish and maintain policies to ensure compliance with the Data Protection Act, GDPR, Human Rights Act, Freedom of Information Act and the common law duty of confidentiality and associated guidance (See Appendix A).
- Information governance training will be mandatory for all staff. This will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. Information governance will be included in induction training for all new staff. The necessity and frequency of any further training will be Personal Development Review (PDR) based.
- The CCGs will undertake annual assessments and audits of their compliance with legal requirements as part of the annual assessment against the IGT standards and in line with changes and developments in legislation and guidance.
- The CCGs have worked with partner NHS bodies and other agencies to establish an Information Sharing Protocol to inform the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Data Protection Act, GDPR, Crime and Disorder Act, Children Act).

- The CCGs will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

6.3 Information Security

- The CCGs will establish and maintain policies for the effective and secure management of their information assets and resources.
- The CCGs will undertake annual assessments and audits of their information and information technology security arrangements as part of the annual assessment against the Information Governance Toolkit standards and in line with changes and developments in legislation and guidance.
- The CCGs will promote effective confidentiality and information security practice to their staff through policies, procedures and training.
- The CCGs have established and maintained incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

  All information governance and IT related incidents, including cyber security incidents (including but not limited to, physical destruction or damage to the organisations computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported to the Information Commissioner's Office (ICO) without delay and no longer than 72 hours and managed through the CCGs Incident Management and Reporting Policy. In addition to the above incidents should be:

  - Notified immediately to the CCGs SIRO and Caldicott Guardian
  - Reported to the Department of Health, Information Commissioner's Office and other regulators via STEIS and the Incident reporting tool
  - Investigated and reviewed in accordance with the guidance in the checklist
  - Reported publicly through the CCGs Annual Report and Governance Statement

- The CCGs will appoint a Senior Information Risk Officer and assign responsibility to Information Asset Owners to manage information risk. A SIRO report will be issued to the Audit and Governance Committee as part of the Information Governance Report.

- The CCGs will appoint a Data Protection Officer (DPO) who has the professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. These are:

- To inform and advise the organisation and its employees 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 assigning responsibilities, managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To cooperate with the supervisory authority (the ICO in the UK);
- To act as the contact point for the supervisory authority and for individuals whose data is processed (employees, patients etc.).

- Under GDPR, the role of DPO is protected and the organisation must ensure that:
  - The DPO reports to the highest management level of the organisation – i.e. Governing Body level.
  - The DPO operates independently and is not dismissed or penalised for performing their task.
  - Adequate resources are provided to enable DPOs to meet their GDPR obligations.

- The CCGs will use pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information.

- The CCGs will conform to developing guidance from NHS Digital and NHS England.

6.4 Clinical information assurance, quality assurance and records management

- The CCGs will establish and maintain policies for information quality assurance and the effective management of records.

- Audits will be undertaken or commissioned of the CCGs' quality of data and records management arrangements.

- Managers will be expected to take ownership of, and seek to improve, the quality of data within their services.

- Wherever possible, information quality will be assured at the point of collection.

- The CCGs will promote data quality through policies, procedures/user manual and training.

- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisations to address the privacy concerns

and risks a technique referred to as a Data Privacy Impact Assessment (DPIA) must be used.

- The CCGs have established a Records Management Policy covering all aspects of records management and consistent with the NHS records Management Code of Practice.

7. TRAINING

7.1 Training

Mandatory Information governance training forms part of induction process and is contractually mandated that all staff complete Mandatory Information governance training annually.

The CCGs have established an IG Training Strategy that identifies the information governance training needs of key staff groups taking into account role, responsibility and accountability levels and will review this regularly through the PDR processes.

8. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Audit and Governance Committee this policy will be disseminated to staff via the CCG's intranet and communication through in-house staff briefings/bulletins.

This policy will be reviewed every year or in line with changes to relevant legislation or national guidance.

9. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the IGT, will be undertaken each year. This includes confidentiality and data protection. Incidents are reported and all serious information governance issues must be reported by the DPO and/or SIRO at Governing Body level and in Annual Reports. Any suspicion of fraud or bribery should be reported at the earliest available opportunity by contacting the CCG Counter Fraud Specialist or via the NHS Protect fraud reporting website Here.

10 ASSOCIATED DOCUMENTS
(Policies, protocols and procedures)

The IG policy and framework should be read in conjunction with the Information Governance Handbook which has been shared with all staff and for which new

staff will be required to sign a receipt saying that they have received and read the Handbook. (see Appendix C)

The CCGs have produced appropriate procedures and guidance related to information governance as required by the below policies:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Integrated Risk Management Framework Incident Reporting Policy
- Business Continuity Policy
- Disciplinary Policy
- Anti-Fraud, Bribery and Corruption Policy Raising Concerns Policy
- Internet and Social Media Policy

And their associated procedures (including but not limited to):

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- Internet and Social Media Policies
- Privacy Impact processes
- Remote access and home working procedures
- Safe Transfer Guidelines and Procedure
- Incident Management, Investigation and Reporting

11 Public Sector Equality Duty

The Equality Act 2010 includes a general legal duty to:

- Eliminate unlawful discrimination, harassment victimisation and any other conduct prohibited under the Act
- Advance quality of opportunity between people who share a protected characteristic and people who do not share it
- Foster good relations between people who share a protected characteristic and people who do not have it

The protected characteristics are:

- Age
- Disability
- Gender reassignment
- Marriage or civil partnership

- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

Public bodies have to demonstrate due regard to the general duty. This means active consideration of equality must influence the decisions reached that will impact on patients, carers, communities and staff.

It is no longer a specific legal requirement to carry out an Equality Impact Assessment on all policies, procedures, practices and plans but, as described above, the CCGs do need to be able to demonstrate they have paid due regard to the general duty.

The policy sets out the CCGs' overall approach to the management of information governance. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

Appendix A

Legislation & Guidance

- Data Protection Act
- General Data Protection Regulation (GDPR)
- NHS Act 2006
- Human Rights Act 1998
- Computer Misuse Act 1990
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Health and Social Care Act 2012
- Crime and Disorder Act 1998
- The Children Act 1989 and 2004Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- NHS Sexually transmitted disease regulations 2000
- Human Fertilisation & Embryology Act 1990
- Abortion Regulations 1991
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health & Safety at Work Act 1974
- Health and Social Care Act 2012
- Public Records Act 1958
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Coroners and Justice Act 2009
- Bribery Act 2010
- Fraud Act 2006
- Caldicott Review updated 2013
- Health and Social Care Information Centre Guidance
- Professional Codes of Conduct and Guidance
- Information Commissioners Guidance Documents
- Health and Social Care (Safety and Quality) Act 2015

This is not an exhaustive list and further guidance can be obtained from your organisation's Caldicott Guardian, Senior Information Risk Owner (SIRO) or the Embed Health Consortium Information Governance Support Team.

Appendix B

CALDICOTT GUARDIAN ROLE SPECIFICATION AND IMPLEMENTATION PLAN

In accordance with the IGT requirements, the Caldicott Guardian role has been established to support the Caldicott Guardian. The Caldicott Guardian is required to be at director level and have a clinical background. The CCGs 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 CCGs staff intranet. This role will be primarily supported by the NHS Code of Confidentiality.

The Caldicott Guardians will be supported by the CCGs IG lead with additional support available from Embed Health Consortium IG team on issues concerning data protection and will provide advice on the release of information to the Police and other agencies as appropriate.

Where CCG and Embed Health Consortium staff processing personal confidential data on behalf of the CCG 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.

Caldicott Issues Log -any incidents relating to patient confidentiality will be recorded and monitored through the existing CCG incident management system. Other patient confidentiality or information sharing issues will be managed by the Caldicott function and, where necessary, escalated to Caldicott Guardian and recorded on the Caldicott Issues Log, the IG lead will support the Caldicott Guardian to ensure that the CCGs benefit from lessons learned by sharing with senior managers and, where relevant, within appropriate CCG quality and governance committees.

Appendix C: Information Governance Declaration Form

I confirm that I have received the **Information Governance User Handbook** and understand that it is my responsibility to read and understand it and to raise any queries or concerns with my line manager or directly with the Embed Health Consortium Information Governance Team (eMBED.infogov@nhs.net).

This booklet has been developed to ensure that users are compliant with, but not limited to, the Data Protection Act (DPA), General Data Protection Regulation (GDPR), Freedom of Information Act 2000, Human Rights Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patent Act 1988, ISO27001 (formerly BS7799) and the Caldicott principles.

It is **IMPORTANT** to remember that **you** are accountable for your computer login and that all activity is auditable. Monitoring of email and internet activity is also carried out. It is **your** responsibility to ensure that only you know your password and that if you leave your PC logged in and unattended you must lock your PC (Press Ctrl+ Alt + Del) to stop any unauthorised use of your PC.

If you choose to make a note of any Login IDs and/ or passwords that you are using, **lock them away in a secure place**. Keep all passwords secure and **DO NOT** disclose them to anyone.

You should be aware that inappropriate use, including any violation of this policy may result in the withdrawal of the facility and may result in prosecution, fines and / or disciplinary action, including dismissal, in accordance with the CCG's disciplinary procedures and GDPR legislation.

Signed:	Date:
Name (Please Print):	
Job Title:	
Team:	
Contact Telephone Number:	

When signed this declaration will be held on your personal file.