CCGs working together

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

CONFIDENTIALITY AND DATA PROTECTION POLICY
(Incorporating the Confidentiality Code of Conduct)

Policy approved by: Audit and Governance Committees

Date: 9th October 2017

Next Review Date: September 2019

Version: 3.0

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Officer
Clinical Lead:	Director of Quality and Nursing
Author:	Senior IG Specialist, eMBED
Date Approved:	9th October 2017
Committee:	Audit and Governance Committee
Version:	3.0
Review Date:	October 2019

Version History

Version no.	Date	Author	Description	Circulation
1.0	27 August 2014	IG Specialist, YHCS	Initial Draft	
2.0	22 September 2016	Senior IG Specialist, eMBED	Reviewed and updated	
2.1	24 August 2017	Senior IG Specialist, eMBED	Reviewed and updated • Combined 3CCGs policy • GDPR update	Head of Governance (initial drafts), A&G Comms (final)
3.0	October 2017	Senior IG Specialist, eMBED	Approved by Audit and Governance Committees 9th October 2017	

Contents

1. INTRODUCTION

NHS Airedale, Wharfedale and Craven Clinical Commissioning Group, Bradford City Clinical Commissioning Group and NHS 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.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified. It is essential that all staff and contractors of the CCGs are fully aware of their personal responsibilities for information which they may come into contact with.

2. AIMS

The aim of the policy is to ensure that all staff understand their obligations with regard to any information they come into contact with in the course of their work and to provide assurance to the governing bodies that the CCGs have in place the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively.

The CCGs will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) (from 25th May 2018), Data Protection Act and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit.

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

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, Governing Body members, Clinical Board, Clinical Executive, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCGs. The policy is applicable to all areas of the organisations and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

All aspects of information within the organisations, 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, mobile storage devices, 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

Confidentiality and data protection within an independent contractor's (such as GPs and dentists) premises is the responsibility of the data controller (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.

The CCGs recognise the changes introduced to information management as a result of the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015 and work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and, where necessary, referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key information governance roles and bodies that the CCGs need to have in place as part of its Information Governance Framework, these are:

- Governing Body
- Audit and Governance Committee
- Accountable Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Information Asset Administrator
- Heads of service
- All employees

The accountability and responsibility are set out in more detail in the Information Governance Strategic Vision, Policy and Framework which must be read in conjunction with this policy.

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

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

'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. CONFIDENTIALITY GUIDANCE AND LEGISLATION

For personal and confidential information held by the CCGs there will be appropriate measures to ensure confidentiality and security, underpinning the principles of Caldicott, Health and Social Care Information Centre Guidance, Information Commissioners Office (ICO) and professional Codes of Practice, legislation and common law.

6.1 General Data Protection Regulations (Regulation (EU) 2016/679) (GDPR)

The GDPR were adopted by the EU in May 2016 and will be implemented in full by 25 May 2018. The GDPR will replace the previous Directive 95/46/EC on which the Data Protection Act was based. All organisations must ensure they are fully compliant within the implementation period. (See Appendix A)

It is important to note that the regulation specifies that:

- a personal data breach' is defined in the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed"
- all actual information breaches must be reported via the IG Toolkit (to the ICO) within 72 hours of becoming known by the data controller.
- data processors must report the incidents to the data controller without undue delay after becoming aware of it; data processors can be held liable for breaches.
- the penalty for breach of the regulations is now capped at a maximum of €20,000,000 or 4% of the turnover of an organisation
- organisations must employ the 'privacy by design' approach to activities involving personal data; a Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- fair processing notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU
- the consent model for processing personal data is to be further defined (see Caldicott 3 report and corresponding consultation and direction from the Department

of Health)

- as part of the implementation of the regulations, a register of data controllers, will no longer be maintained by the ICO and organisations will not be required to complete/renew an annual submission
- data subjects have the new right to erasure, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within 30 days and provided free of charge (unless a request is "manifestly unfounded or excessive")

6.2 Data Protection Act

All information and data which can identify a living person, held in any format (visual, verbal, paper, electronic, digital, microfilm, etc) is safeguarded by the Act, which is underpinned by eight principles. (See Appendix B)

The Act is enforced by the ICO. Fines can be made against organisations or persons holding personal information (data controllers) of up to £500,000 where is a serious breach of the Act e.g. loss of personal data of many individuals.

The Act requires data controllers such as the CCGs to register on an annual basis with the ICO (Register of data controllers) until May 2018, after which this is no longer a requirement.

6.3 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

6.4 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented
- Where disclosure is in the public interest; and
- Where there is a legal duty to do so, for example a court order

6.5 Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure. She was asked to conduct a further review and a new report: 'Information to share or not to share' was published in March 2013. The recommendations of this report have been largely accepted by the government and a revised set of Caldicott Principles were published (See Appendix C)

The Caldicott Guardian also has a strategic and operational 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. A detailed description of the Caldicott Function is given in the Information Governance Strategy.

6.6 NHS Digital (Health and Social Care Information Centre) Guidance

This organisation was established in April 2013 and is responsible for facilitating the management and sharing of data across the NHS to support both operational and other functions such as planning, research and assessments. HSCIC produced a Code of Practice: 'A Guide to Confidentiality in Health and Social Care' in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

6.7 The NHS and Social Care Record Guarantees for England

The NHS and Social Care Record Guarantees for England sets out the rules that govern how individual care information is used in the NHS and in Social Care. It also sets out what control the individual can have over this.

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

6.8 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' refer to approval given under the authority of the Regulations.

The Health Research Authority (HRA) took on responsibility for Section 251 in April 2013, establishing the Confidentiality Advisory Group (CAG) function.

6.9 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

6.10 Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which are relevant to data protection and confidentiality which may have an effect on disclosure and use of information (see list below). This is not an exhaustive list. Where you need any further guidance regarding any of the legislation or guidance listed - you can contact the organisations Caldicott Guardian, the Senior Information Risk Owner (SIRO) or the Information Governance lead (see section 11 Advice and Guidance).

- Abortion Regulations 1991
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- National Data Guardian report
- Health and Social Care Act 2012
- Human Fertilisation and Embryology Act 1990
- NHS Sexually transmitted disease regulations 2000
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012

- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004
- NHS Digital. "FAQs on legal access to personal confidential data." Accessed 16 September 2016. Available from http://digital.nhs.uk/article/3638/Personal-data-access-FAQs.

All staff are bound by the codes of conduct produced by any professional regulatory body, by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

7. ENSURING INFORMATION IS SECURE AND CONFIDENTIAL

7.1 General principles

- The CCGs regard all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework 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 and procedures to ensure compliance with the General Data Protection Regulation (from 25th May 2018), Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality and the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable confidentiality and data protection controls are in place.
- Where any disclosure of PCD is made there a must be a legal basis for doing so.

7.2 Using and disclosing confidential patient information for direct healthcare

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct healthcare but patients should still be informed about:

- The use and disclosure of their healthcare information and records.
- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.

- The potential use of their records for the clinical governance and audit of the care they have received.
- Through a privacy notice outlining what information will be shared, the purpose of this, who the data will be shared with, how long data will be retained, the rights of the data subject (including opt-outs) and what security measures are in place to protect confidentiality.
- If not for direct care then explicit consent or some other legal basis must be present to enable sharing.

7.3 Using and disclosing confidential staff information

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct communications related to their role, salary payment and pension arrangements. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of Freedom of Information requested where the public interest in disclosure is deemed to override confidentiality considerations.

Using staff information for other purposes must be subject to explicit consent being granted unless another legal basis permits this.

7.4 Using and disclosing corporate and business information

All staff should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes.

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 Scheme.

7.5 Information security

Rules and guidance on information security are set out in

- **The Information Security Policy** - sets rules, guidance and good practice on ensuring security of information in the workplace, on areas such as portable devices, email, paper and electronic systems.
- **The Records Management and Information Lifecycle Policy** – includes sections on transfer of, storage and archival of records.

7.6 Sharing confidential information without consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. Safeguarding children concerns) or a court order must be in place. In deciding on any disclosure certain considerations and steps need to be taken:

- Discuss the request with the appropriate CCG personnel such as the Caldicott

Guardian and/or SIRO.

- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- Follow any locally agreed Information Sharing Protocols and national guidance.

Requests may be received by other agencies which are related to law enforcement such as:

- The police or another enforcement agency where the appropriate section 29 request form (in line with the Access to Records Procedure) needs to be submitted from the law enforcement agency in order for the CCGs to consider the request.
- The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Staff should also take into account the seventh Caldicott principle if there is a clear legal basis to share: '*The duty to share information can be as important as the duty to protect patient confidentiality'.*

7.7 Confidentiality and conversations

Where during the course of your work you have conversations relating to confidential matters which may involve discussing (or disclosing information about) individuals such as staff members or patients you must ensure:

- That such discussions take place where they cannot be overheard.
- That for telephone calls the rule is you do not give out confidential information over the phone - unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak with another team member on the phone who is based at another location).
- Where you receive a request over the telephone for confidential information ask the caller to put the request in writing so details can be verified.
- That you do not discuss confidential work matters in public places or at social occasions.
- Where an answer phone is used ensure that recorded conversations on the phone phones cannot be overheard or otherwise inappropriately accessed.

7.8 Records management

The CCGs have a Records Management and Lifecycle Policy which should be followed for all aspects of record creation, sharing, storage, retention and destruction of records.

7.9 Access to records

Individuals have a right to request access to their records in line with the Data Protection Act and the General Data Protection Regulation (from 25th May 2018) by making a

Subject Access Request. All staff should familiarise themselves with the CCGs' Access to Records Procedure which should be followed for all requests for personal data. This procedure also gives guidance in relation to requests for the records of deceased persons' under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

Access to corporate information and records will be in accordance with CCG Freedom of Information Act and Environmental Information Regulations Policy.

7.10 Information sharing

The organisations will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Code of Conduct and in accordance with the Health and Social Care Act 2012.

Any local Information Sharing Protocols that the CCGs are signed up to need to be followed at all times.

7.11 Information confidentiality breaches

All information governance and IT related breaches, including cyber security breaches (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.

Breaches should be:

- Notified immediately to the CCGs Governance team, SIRO and Caldicott Guardian
- Reported to the Department of Health, Information Commissioner's Office and other regulators via STEIS and the Incident Reporting Tool (external reporting will be co-ordinated by the CCG Governance team).
- Investigated and reviewed in accordance with the guidance in the checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

What should be reported?

Misuses of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. The following list gives some examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential personal information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act, General Data Protection Regulation (from 25th May 2018), and NHS Code of Confidentiality.
- Sending data in a way that breaches confidentiality.
- Leaving confidential information lying around in a public area e.g. photocopier.
- Theft or loss of patient-identifiable information.
- Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient records and or content of in an ordinary waste paper bin

7.12 Privacy Impact Assessment

All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns and risks a technique referred to as a Data Privacy Impact Assessment (DPIA) must be used and will be mandated by law from (from 25th May 2018),. A DPIA will:

- Identify privacy risks to individuals
- Protect the CCGs' reputation
- Ensure person identifiable data is being processed safely
- Foresee problems and negotiate solutions

The CCGs' procedure for DPIA should be followed.

8. TRAINING

8.1 Mandatory training

The Information Governance Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance in accordance with the IG Training Strategy.

Training will be primarily delivered online through the learning and development service offered by the Bradford District Care Trust (BDCT).

Managers must actively ensure that **all** staff undertake and complete the mandatory information governance training.

8.2 Specialist training

Additional training may be provided in specialist areas such as data protection. The need for additional training should be identified with reference to the IG Training Strategy.

9. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Audit and Governance Committee this policy will be disseminated to staff via the CCGs' intranets and communication through in-house staff briefings.

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

10. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Information Governance Toolkit (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 SIRO at Governing Body level and in Annual Reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the report NHS fraud website.

11. ADVICE AND GUIDANCE

Advice and guidance on any matters stemming from the policy can be obtained by contacting:

EMBED.Infogov@nhs.net

12. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

This policy should be read in conjunction with:

- 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 FrameworkIncident 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
- Privacy Impact processes
- Remote Access and Home Working Procedures
- Safe Transfer Guidelines and Procedure

Incident Management, Investigation and Reporting Procedures
This policy should be read in conjunction with the Information Governance Handbook which has been shared with all staff and for which new staff will need to sign for receipt and confirm that they have read the document. (see Appendix D)

13. 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.

This policy sets out how the CCGs ensure that information is managed legally, efficiently and effectively. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

Appendix A

General Data Protection Regulation principles:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

It is important to note that the regulations specify that:

- data processors can be held liable for breaches
- all actual information breaches must be reported via the IG Toolkit (to the ICO) within 72 hours of becoming known
- the penalty for breach of the regulations is now capped at a maximum of €20,000,000 or 4% of the turnover of an organisation
- organisations must employ the 'privacy by design' approach to activities involving personal data. A Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- fair processing notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU

- the consent model for processing personal data is to be further defined (see Caldicott 3 report and corresponding consultation and direction from the Department of Health)
- as part of the implementation of the regulations, a register of data controllers, will no longer be maintained by the ICO and organisations will not be required to complete/renew an annual submission
- data subjects have the new right to erasure, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within 30 days and provided free of charge (unless a request is “manifestly unfounded or excessive”)

Appendix B

Data protection Act principles:

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

Appendix C

Caldicott principles:

1. *Justify the purpose(s)*
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.
2. *Don't use personal confidential data unless it is absolutely necessary*
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. *Use the minimum necessary personal confidential data*
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. *Access to personal confidential data should be on a strict need-to-know basis*
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. *Everyone with access to personal confidential data should be aware of their responsibilities*
   Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. *Understand and comply with the law*
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. *The duty to share information can be as important as the duty to protect patient confidentiality*
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix D

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 Information Governance Team EMBED.Infogov@nhs.net

This booklet has been developed to ensure that users are compliant with all relevant legislation and guidance including, but not limited to, the Data Protection Act (DPA), General Data Protection Regulation (from 25th May 2018), 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 and / or disciplinary action, including dismissal, in accordance with the CCG's disciplinary procedures.

Signed:	Date:
Name (Please Print):	

Job Title:
Team:
Contact Telephone Number:

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