Newcastle Gateshead
Clinical Commissioning Group

Corporate	CCG: IG01: Confidentiality and Data Protection Policy

Version Number	Date Issued	Review Date
V3	July 2018	July 2020

Prepared By:	Senior Governance Officer (IG), NECS
Consultation Process:	CCG Head of Corporate Affairs CCG Quality, Safety & Risk Committee NECS IG Team

Policy Adopted From:	IG01: V2.1 Confidentiality and Data Protection Policy
Approval Given By:	Quality, Safety & Risk Committee

Document History

Version	Date	Significant Changes
1	28/02/2013	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
2	03/02/2015	Policy refresh in line with changing CCG incident reporting and management requirements aligned to the introduction of Safeguard Incident Risk System (SIRMS) across the CCG.
2.1	17/10/2017	Review and update to include GDPR
3	May 2018	Amended following publication of the Data Protection Act 2018

Equality Impact Assessment

Date	Issues
June 2018	Please see Section 9 of this document

Policy Validity Statement
This policy is due for review on the latest date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Contents

1. Introduction

The CCG aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

This policy relates to the processing of personal information and to the management of personal information about staff, patients/service users. The CCG is required by law to comply with the Data Protection Act 2018, which is concerned with the lawful processing of information relating to living individuals.

Note: The UK Data Protection Legislation incorporates the European Union General Data Protection Regulation (GDPR) which was adopted by the European Union in 2016,.

To comply with the law staff or others who process personal information must ensure they follow the Data Protection Principles and the Caldicott Principles. The obligation to keep information confidential arises out of the common law duty of confidentiality, professional obligations and staff /third party contracts. The NHS code of Practice: Confidentiality provides guidance to the NHS and related organisations. These duties and obligations mean that all staff with access to confidential personal information must keep that information safe and secure.

1.1 Status

This policy is an Information Governance policy.

1.2 Purpose and scope

This policy sets out the CCG's commitment to the confidentiality of personal information and its responsibilities with regard to the disclosure of such information.

It aims to ensure all staff whether directly employed or contracted are aware of their responsibilities towards the confidentiality of personal information.

This policy applies to all organisation staff including temporary and agency, contractors and volunteers and to personal information recorded in any format, including paper, electronic and any other medium e.g. images.

2. Definitions

2.1 **Confidentiality:** the ethical principle or legal right that a physician or other health and social care professional will hold secret all information relating to a patient/service user, unless they have given informed consent permitting disclosure.

2.2 **Data:** information as defined by the DPA 2018 which:

- Is processed electronically i.e. information systems, databases, microfiche, audio and video systems (CCTV) and telephone logging systems.
- Is recorded with the intention that it shall be processed by equipment.
- Is recorded as part of a relevant filing system i.e. structured, either by reference to individuals or by reference to criteria relating to individuals which is readily accessible.

2.3 **Data Controller:** the individual, company or organisation who determines the purpose and the manner in which personal data may be processed. The Data controller is the CCG.

2.4 **Data Processor:** any person other than an employee of the Data Controller who processes data on behalf of and/or under the instruction of the Data Controller.

2.5 **Data Subject:** a living individual who is the subject of the personal data.

2.6 **Disclosure:** the divulging or provision of access to data.

2.7 **Personal Information:** personal information which relates to a living individual who can be identified from that information or from that information and other information which is in the possession of, or likely to come into the possession of the data controller

2.8 **Processing:** using information in the following ways;

- Obtaining
- Recording
- Retrieving
- Altering
- Disclosing
- Destroying
- Using
- Transmitting
- Erasing
- Storing / Archiving
- Sharing

Or, in other words, anything you do with data is processing.

2.9 **Sensitive Personal Data:** also known as 'Special Category Data' as set out in the DPA 2018 is any information about a person relating to their;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Biometric Data
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed

2.10 **Third Party:** any person other than:

- The data subject
- The data controller
- Any data processor or other person authorised to process data on behalf of the data controller

Note: The key terms used in the GDPR are largely consistent with the 1998 Act but the draft UK Data Protection Bill makes use of derogations where it is possible to achieve further consistency.

3. Confidentiality of Personal Information and Data Protection

3.1 Duty of Confidentiality

3.1.1 All staff and contractors must recognise that confidentiality is an obligation. Any breach of confidence, inappropriate use of records or abuse of computer systems may lead to disciplinary procedures, bring into question professional registration and may result in legal proceedings.

3.1.2 Agency/temporary and voluntary staff are also subject to such obligations and must sign a confidentiality agreement as appropriate when working for or on behalf of the CCG.

3.1.3 Generally, there are five main areas of law which govern the use and disclosure of confidential information. These are briefly described at Appendix A but are covered in more detail in the Department of Health document Confidentiality: Code of Practice for Health and Social Care 2016.

3.2 The Caldicott Principles for Protecting and Using Personal Information

3.2.1 The Caldicott Committee Report on the Review of Patient-Identifiable Information 1997 found that compliance with confidentiality and security arrangements was patchy across the NHS and identified six good practice principles for the health service when handling patient information. These principles can be extended to also apply to social care service user information. A further Caldicott2 review was published in March 2013 which amended the Caldicott Principles, as follows;

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality.

Further explanation of the revised Caldicott Principles can be found at Appendix B.

3.3 The Role of the Caldicott Guardian

3.3.1 The Caldicott Committee Report also led to the appointment of Caldicott Guardians for each NHS organisation. Their role (see also Duties section) is to oversee how staff use personal information, agree and monitor protocols for sharing information across organisational boundaries, ensure that patient's/service user's rights to confidentiality are respected and to safeguard the security of personal information. Further information is available in the Information Sharing & Disclosure Procedures.

3.4 The Data Protection Principles

3.4.1 The Data Protection Act 2018 applies the six Data Protection Principles under GDPR to support good practice and fairness in processing personal information. These principles stipulate that personal data shall be:

- Fairly, transparently, lawfully processed
- Processed for limited and specific purposes
- Adequate, relevant and not excessive (i.e. minimised)
- Accurate and up to date
- Not kept longer than necessary
- Securely held with integrity and confidentiality

The GDPR also specifically outlines new rights for data subjects and addresses the transfer of data to countries outside of the EEC separately to the principles.

GDPR also introduces a principle of Accountability.

Further explanation of the Data Protection Principles can be found at Appendix A.

3.4.2 The Act requires the CCG to register or 'notify' as a data controller with the Office of the Information Commissioner detailing the purposes for which personal information is used, and use of data beyond that specified in the registration is unlawful. This notification must be regularly reviewed and any changes made within 30 days of the date on which the entry became inaccurate or incomplete. An annual fee is paid to the Information Commissioner's Office (ICO) to maintain notification on the ICO register.

Note: The GDPR does not require notification with the 'supervisory authority' however the UK Data Protection Act 2018 provides the Secretary of State with a power to make regulations requiring data controllers to pay a charge to the ICO.

3.5 Disclosure of Personal Information

3.5.1 Whether personal information can be disclosed to others is dependent on a number of factors, including, whether the patient/service user has consented to the information being shared, to whom the information is being disclosed and the reason for its disclosure. There are a number of considerations to be made when deciding whether or not to disclose information. The approach may vary according to the individual circumstances surrounding the disclosure. For example the considerations in disclosing personal information to the police will be different to those in disclosing information for research purposes. These are explained further in the Information Access Policy.

3.6 Information Security

3.6.1 In order to ensure the confidentiality of personal information, systems and procedures are in place to control access to such information. Such controls are essential to ensure that only authorised persons have:

- physical access to computer hardware and equipment,
- access to computer system utilities capable of overriding system and access controls e.g. administrator rights,
- access to either electronic or paper records containing confidential information about individuals

3.6.2 The arrangements for the security of computer hardware, system utilities, computer files and folders is set out in the Information Security Policy and related procedures. The policy contains guidance on access controls, encryption of data, user responsibilities, security monitoring and security incidents.

3.6.3 For further guidance on maintaining the confidentiality and security of personal information whilst in transit please refer to the Information Security Policy.

3.7 Risks and Incidents

3.7.1 All risks and incidents relating to Confidentiality must be reported using the CCG's standard procedures for risk and incident reporting. The Information Governance and Information Risk Policy provides more guidance on this process.

3.7.2 Reporting of risks and incidents is important to ensure that appropriate action is taken so that risks/incidents do not reoccur and to learn from them. No constructive action can be taken if the CCG is not notified when things go wrong or there is a near miss.

3.7.3 Serious data breaches must be reported to the ICO under the Data Protection Act 2018 within 72 hours of becoming aware of the breach. The NECS IG Team can provide advise as to what constitutes a serious breach.

3.8 Retention and Storage

3.8.1 Records are to be retained in accordance with the Department of Health's Records management code of practice for health and social care 2016.

3.8.2 Records, whether held in paper or electronic form must be stored securely to prevent unauthorised access. Further information regarding secure storage is available from the Information Security Policy (i.e. access controls) and the Records Management Policy (i.e. storage and retention).

3.8.3 Confidential records should be archived at a secure facility or destroyed in a secure manner, such as use of a confidential shredding company for paper records, or for electronic records held on a hard drive by secure erasing via the ICT department

3.9 Access to Personal Information

3.9.1 Individuals or persons acting on their behalf with consent have a right of access to data held about them. Any person who wishes to exercise this right should make their request to the Information Governance Team.

3.9.2 The process for doing this is in the Information Access Policy.

3.9.3 Under the Data Protection Act 2018 data subjects also have rights have their data, corrected, erased, shared with other organisations, or to have the processing of their data stopped or altered. It should be noted that there are exemptions to some of these rights where medical records or matters of public interest / public health are concerned.

4. Duties and Responsibilities

Governing Body	The Commissioning Forum has delegated responsibility to the Governing Body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents. The Quality, Safety and Risk Committee supports the GB ensuring adequacy and effectiveness of policies and procedures as outlined in the CCG constitution.

Chief Officer	The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Caldicott Guardian	The Caldicott Guardian is responsible for ensuring that national and local guidelines and protocols on the handling and management of personal and sensitive information are in place.
Data Protection Officer	The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and to advise the CCG on their obligations under Data Protection Legislation.
Head of Corporate Affairs (IG Lead CCG)	Responsible for ensuring that operational aspects of IG are undertaken in a timely fashion. • Responsible for reviewing IG policies • Responsible for cascading IG related information to the CCGs staff • Ensures that recommended actions arising from audits are carried out. • Ensures that the CCG's evidence for the IG Toolkit is collated and gathered by the appropriate deadlines • Works with the IG Lead (CSU) to maintain/improve the CCG's IG status
IG Lead(CSU)	Will be responsible for: • Undertaking compliance audits of records management programmes (policies, procedures and systems) to ensure statutory obligations are met including those under the Data Protection Act 1998 (GDPR and UK Data Protection Bill from 25 May 2018) and the Freedom of Information Act 2000. • Issuing guidance for implementing and compliance with this policy. • Encouraging all staff to follow the principles of the Data Protection Act (GDPR and UK Data Protection Bill from 25 May 2018). • Monitoring performance through quality control and internal audits. • Identifying areas where improvements could be made. • Reporting performance standards to the relevant committee. • Monitoring compliance with the standards, legislation, policies and procedures relating to Data Protection. • Monitoring that staff are appropriately trained on records management, confidentiality and data protection. • Ensuring that the ICO Data Protection Notification is kept up to date (no requirement under GDPR).

Line Managers	Managers are responsible for ensuring that their service works within the Data Protection Act (GDPR and UK Data Protection Bill from 25 May 2018). They will ensure that: • There are effective methods for communicating Data Protection related issues. • Staff attend relevant training, induction and mandatory updates in relation to Data Protection. • Staff are aware of and adhere to information governance policies and procedures. • Incident reporting is integral to the operational activities within their areas and all incidents are reported and investigated in accordance with policy. • Information governance issues are discussed at appropriate forums.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided. • Understand and comply with Data Protection Legislation
CSU Staff	Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures.

5. Implementation

5.1 This policy will be available to all Staff for use in relation to the specific function of the policy.

5.2 All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

6. Training Implications

6.1 It has been determined that there are no specific training requirements associated with this policy/procedure. All staff should undertake mandatory data protection training annually.

7. Related Documents

7.1 Other related policy documents

- Information Access Policy
- Information Security Policy

7.2 Legislation and statutory requirements

7.2.1 The Data Protection Act 2018 (DPA) regulates the "processing" of personal data in whatever format including patient/service user identifiable information. Processing refers to anything done with the information including its collection, use (including viewing), disclosure and destruction. The DPA obliges organisations to inform the Information Commissioner that personal information is being processed and to provide data subjects with access to their personal information. The eight Data Protection Principles set out how personal information must be managed (see Appendix C). Note: These principles are largely carried over to the GDPR, which contains six principles and also provides a new accountability principle.

The CCGs responsibilities for confidentiality and appropriate processing of personal data under DPA remain in place even if the processing is being undertaken by a third party contractor or by non-organisation employed staff. Though under the GDPR liability does extend to processors as well as Controllers of data.

7.2.2 The Criminal Justice and Immigration Act 2008 extends the powers of the Information Commissioner under the Data Protection Act 2018 to allow fines of up to £500,000 for individuals or organisations found guilty of deliberate or reckless disclosure of information, including failure to take appropriate security precautions. In addition, individuals can receive a prison sentence on conviction of an offence under DPA and fines from the ICO under GDPR can be up to €20m.

7.2.3 The Common Law Duty of Confidentiality is not written in statute but is based on legal precedent. The common law duty of confidentiality means that information confided by a patient/service user or otherwise obtained (e.g. during medical examination or when receiving personal care), where it is expected that a duty of confidence applies, should not generally be used or disclosed further, except as originally understood by the confider or with their subsequent permission. This duty may be set aside and confidential information disclosed where it is in the public interest or when it is a legal requirement to do so.

7.2.4 Article 8 of the Human Rights Act establishes the right to respect for an individual's private and family life. Current understanding is that compliance with the Data Protection Act 2018 and the common law duty of confidentiality should satisfy these requirements.

Administrative law governs the actions of public authorities to ensure that they operate within their lawful powers. When obtaining or disclosing personal information organisations must demonstrate that it is within the scope of their powers to do so. In general this means that the CCGs may only collect, hold and use information about patients and service users for the purposes of providing those individuals with health or social care services. Unless allowed or required by legislation or unless the common law duty of confidentiality can be set aside, disclosure and/or further use of that information can only take place where consent is obtained.

8. Monitoring, Review and Archiving

8.1 Monitoring

8.1.1 The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

8.2 Review

8.2.1 The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

8.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'version control' table on the first page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

8.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with the Department of Health's Records management code of practice for health and social care 2016.

9. Equality Analysis

North of England Commissioning Support

Partners in improving local health

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	Senior Governance Officer, NECS
Title of service/policy/process:	Confidentiality and Data Protection Policy
Existing: √ New/proposed: □ Changed:	
What are the intended outcomes of this policy/service/process? Include outline of objectives and aims	
This policy relates to the processing of personal information and to the management of personal information about staff, patients/service users. The CCG is required by law to comply with the Data Protection Act 1998 (GDPR/UK Data Protection Bill from May 2018), which is concerned with the lawful processing of information relating to living individuals. The policy compliments other Information Governance policies.	

Who will be affected by this policy/service /process? (please tick)
□ Consultants □ Nurses □ Doctors √ Staff members □ Patients □ Public □ Other
If other please state:

What is your source of feedback/existing evidence? (please tick)
□ National Reports □ Internal Audits □ Patient Surveys □ Staff Surveys □ Complaints/Incidents □ Focus Groups □ Stakeholder groups √Previous EIAs □ Other
If other please state:

Evidence	What does it tell me? (about the existing service/policy/process? Is there anything suggest there may be challenges when designing something new?)
National Reports	N/A
Patient Surveys	N/A
Staff Surveys	N/A
Complaints and Incidents	N/A
Results of consultations with different stakeholder groups – staff/local community groups	N/A
Focus Groups	N/A
Other evidence (please describe)	N/A

STEP 2 - IMPACT ASSESSMENT

What impact will the new policy/system/process have on the following: (Please refer to the 'EIA Impact Questions to Ask' document for reference)
Age A person belonging to a particular age
No impact identified
Disability A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities
No impact identified
Gender reassignment (including transgender) Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self perception.
No impact identified

Marriage and civil partnership Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters
No impact identified
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.
No impact identified
Race It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.
No impact identified
Religion or belief Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.
No impact identified
Sex/Gender A man or a woman.
No impact identified
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes
No impact identified
Carers A family member or paid helper who regularly looks after a child or a sick, elderly, or disabled person
No impact identified
Other identified groups such as deprived socio-economic groups, substance/alcohol abuse and sex workers
No impact identified

STEP 3 - ENGAGEMENT AND INVOLVEMENT

How have you engaged stakeholders in testing the policy or process proposals including the impact on protected characteristics?
No engagement undertaken as this policy has received minor amendments only
Please list the stakeholders engaged:

STEP 4 - METHODS OF COMMUNICATION

What methods of communication do you plan to use to inform service users of the policy?
□ **Verbal – stakeholder groups/meetings** □ **Verbal - Telephone** □ **Written – Letter** □ **Written – Leaflets/guidance booklets** □ **Email** √ **Internet** □ **Other**
If other please state:

ACCESSIBLE INFORMATION STANDARD

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

Tick to confirm you have you considered an agreed process for:
√ **Sending out correspondence in alternative formats.** √ **Sending out correspondence in alternative languages.** √ **Producing / obtaining information in alternative formats.** √ **Arranging / booking professional communication support.** √ **Booking / arranging longer appointments for patients / service users with communication needs.**
If any of the above have not been considered, please state the reason:

STEP 5 - SUMMARY OF POTENTIAL CHALLENGES

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
1	

STEP 6- ACTION PLAN

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date
	None identified.					

Ref no.	Who have you consulted with for a solution? (users, other services, etc)	Person/ People to inform	How will you monitor and review whether the action is effective?
	None identified.		

SIGN OFF

Completed by:	**Alan Clement, Senior Governance Officer**
Date:	**June 2018**
Presented to: (appropriate committee)	**Quality, Safety and Risk Committee**
Publication date:	**July 2018**

Appendix A

Data Protection Act 2018 Principles

Principle 1 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals (data subjects)

Principle 2 Personal Data will only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Principle 3 Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Principle 4 Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Principle 5 Personal data shall be 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.

Principle 6 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

The Accountability Principle (Article 5(2) GDPR)

The controller shall be responsible for, and can demonstrate compliance with the principles – this is referred to as the new accountability principle. The 'Accountability Principle' means Controllers are required to show how they are compliant with the principles – for example by documenting the decisions taken about a processing activity.

Appendix B

Caldicott 2 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. 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 framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix C

Confidentiality Code of Conduct

1. Background

The NHS holds large amounts of confidential information about you, members of your family, friends, and colleagues; but the vast majority of this information will be about strangers, most of whom you are unlikely to meet. This information is classed as personal information and belongs to the individual. Their information should be treated with as much respect and integrity as you would like others to treat your own information. It is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that personal information is not made available to unauthorised persons.

The Code of Conduct is about promoting best practice and continuing improvement in the use of personal health/social care information as an integral part of patient/service user care. Involving patients/service users in decisions about their health/social care information and how it is used is also integral to improving patient/service user confidence in their health/social care services.

Protection of personal health/social care information is part of good practice, and is underpinned by the common law duty of confidentiality, the implementation of the Data Protection Act 2018, GDPR, Codes of Professional Practice, the Human Rights Act 1998 and the Health and Social Care Act 2012. All NHS organisations are registered under the Data Protection Act 2018 (including GDPR) and careless or deliberate misuse of personal information may result in that organisation, and in some cases the individual concerned, being prosecuted under the Act, which may impose fines of up to €20m for serious breaches.

Breaches of confidentiality are a serious matter. Non-compliance with this Code will result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so.

2. Aim of the Document

This document seeks to provide a code of conduct for all staff working in the CCG, which will ensure the confidentiality of personal information at all times.

National guidance and legal implications

National guidance includes the NHS Codes of Practice on Confidentiality & Information Security Management, the Caldicott2 Principles (see below) and the NHS Care Record Guarantee. Care professionals must also comply with codes of practice of their respective professions.

Generally, there are five main areas of law which constrain the use and disclosure of confidential information. These are briefly described below but are covered in more detail in the document, Confidentiality: NHS Code of Practice, 2003 and in the IG policies & procedures.

The Data Protection Act 2018 (DPA)

The DPA is designed to control the use, storage and processing of personal data in whatever format - especially where there is a risk to personal privacy. Patients/service users and staff should be aware that their information will be stored and processed.

General Data Protection Regulations (from May 2018)

The European Union General Data Protection Regulation (GDPR) which was adopted by the European Union in 2016, cameinto force in all EU Member States from 25 May 2018, combined with the Data Protection Bill they received Royal assent in 2018 to become the UK's new Data Protection Legislation – The Data Protection Act 2018. The new law aims to protect privacy, strengthen rights and empower individuals to have more control over their personal data by providing easier access. Individuals will generally have more control over their digital footprint, their personal data, how it is used and passed on by companies.

Common law of confidentiality

Although not written in statute, the principle of the common law of confidentiality states that information confided should not be used or disclosed further, except as originally understood by the confider, or with her/his subsequent permission. In other words, if you are told something in confidence, you are not at liberty to disclose the information without permission unless required by law to do so.

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Health and Social Care Act 2012

This Act introduced changes regarding access to patient confidential data and placed particular restrictions on access to patient data by commissioning organisations and their support organisations.

Administrative law

Administrative law governs the actions of public authorities to ensure that they operate within their lawful powers. In other words, the authority must possess the power to carry out what it intends to do and is particularly relevant to the issue of patient consent.

Users' rights

Patients/service users and families have a right to believe and expect that private and personal information given in confidence will be used for the purposes for which it was originally given, and not released to others without their consent. Everyone in the NHS must safeguard the integrity and confidentiality of, and access to sensitive information.

3. Definitions

The Code relates to personal information as defined within the IG policies & procedures which includes staff information that is personal.

Who is an unauthorised person?

Your job role, or level of access to a computer system, provides you with a level of authority to access information. Do not assume that all your work colleagues are authorised to see the same information that you are. Even if they are in a more senior role to you - if they do not need to know the information, they do not need to have it. If you are in doubt as to whether you should share the information with one of your colleagues, seek the advice of your manager or the NECS Information Governance service.

What is meant by the transfer of personal information?

The transfer of personal information, by whatever means, can be as simple as:

- taking a document and giving it to a colleague;
- making a telephone call;
- sending a fax;
- passing on information held on computer, for example confidential clinical information held on patient records.

In all cases, however simple or complicated, the Caldicott2 Principles must be adhered to in order to ensure that personal information is not disclosed inappropriately.

Caldicott 2 Principles

1. Justify the purpose(s).
2. Don't use personal confidential data unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

4. Ensuring Confidentiality

Physical security

Personal information should always be held securely and should never be left unattended. In any area which is not secure, and which can be accessed by a wide range of people (including possibly visitors to the premises), such information should be put/locked away immediately after it has been finished with. Care must be taken to ensure that any personal information cannot be viewed by visitors to the area and that staff are aware of and adhere to the organisational security procedures.

Safeguarding information

- Never leave personal information around for others to find.

- Wherever possible, avoid taking confidential information away from your work premises. Where this is necessary in order to carry out your duties you must keep the information secure and make every effort to ensure that it does not get misplaced, lost or stolen.

Remember - you are bound by the same rules of confidentiality while away from your place of work as when you are at your desk.

- When disposing of personal information in paper form, ensure that it disposed of in accordance with the Disposal of Confidential Waste Procedures. Never put confidential information directly into a general waste paper bin.
- Work diaries can hold a great deal of personal information and should be kept secure when not in use. Precautions should be taken when transporting your work diary to ensure it is in your care at all times. Remember to hand back any work diaries at the end of each calendar year.
- If documents containing personal information come into your possession and you are not the intended recipient, you should report this as an information governance incident on the incident reporting system. Appropriate action should be taken to resolve the issue and advice may be sought from the NECS Information Governance service.

- Always ensure that documents are labelled with a security marking appropriate to the contents. Advice on security markings may be sought from the CSU Information Governance service.

Information transfer

It is imperative that the utmost care is exercised when transferring personal information. The basic rule is that in all circumstances where personal information is shared, by whatever method, the items transferred should be restricted to a minimum. The following key points should be considered:

- Always consider the most appropriate method of transferring personal information and taking account of the Caldicott2 principles.
- Always encrypt information transferred electronically (e.g. by email or on removable media) appropriately.
- Always adopt 'safe haven' principles to ensure confidentiality when transferring information:
    - Sort and store post away from public areas, in rooms which are either locked or secured by key pads
    - Place health or social care records face down, do not leave unsupervised in public areas or on desks or in trays for long periods of time
    - Protect answer machines pin number (if possible) and locate in rooms which are either locked or secured by key pads
    - Fax machines sited away from public areas in rooms which are either locked or secured by key pads (see below for fax safe haven guidance)
- Check that the contact details for the recipient are correct before transferring personal information (e.g. address, email address, fax number); use appropriate cover sheets for confidential faxes and confirm receipt.
- Always package personal information securely before transferring by post or courier, mark the package as private & confidential and, wherever possible, uses a secure postal service (e.g. Royal Mail Special Delivery). Write a return address on the back of the envelope (if it doesn't compromise confidentiality).
- Consider carefully the possible risks involved in using telephones or texting for sharing personal information.
- When transferring information in person ensure information is out of sight e.g. in boot of car, in a bag if travelling on public transport.

If information is going to be transferred between organisations on a regular basis, it is good practice to have an Information Sharing Agreement in place. Further advice on information sharing agreements can be sought from the CSU Information Governance service.

Indiscreet conversations

- Ensure you cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about confidential information. In these situations, if you do not need to identify a patient/service user by name, do not do so.
- It is not appropriate to discuss personal information in hallways, corridors or stairways or any other public place where you might be overheard.
- When speaking to a patient/service user or carer on the telephone, confirm the caller's identity or ring back. If in doubt, ask for confirmation in writing, or by fax.

Inappropriate sending of faxes

Use of fax machines should be avoided unless absolutely necessary. When sending faxes that contain personal information apply safe haven principles as follows:

- Telephone first to inform the recipient that you are faxing confidential information.
- Ask them to wait by the fax machine whilst you send it.
- Ask them to telephone to acknowledge receipt.
- Always double check that you have keyed in the right number before hitting the "send" key.
- Numbers used regularly should be programmed (& tested) into your fax machine, so decreasing the possibility of keying in the wrong number.

Safeguarding electronic information

The security and confidentiality of information held on computer must be maintained at all times.

- Never leave a computer logged on to a system and unprotected. Always protect the system (e.g. log off or use a password-protected screensaver) when you have finished or stop using it for a period. Always log off when you have finished. Failure to do this not only leads to a risk of unauthorised access to personal information, but you will be held responsible for any actions associated with your sign-on.
- Do not walk away from your work area and leave personal information on your screen for unauthorised persons to see. If you need to leave your desk, you should protect the system (e.g. log off or use a password-protected screensaver).
- Never save information on to the hard drive (C:\) of a computer.
- Always remove your Smartcard from your computer (if using one to access systems) when leaving your workstation.

- Passwords are the keys that provide access to information; you must not disclose your network password to anyone under any circumstances. If you have to write your password down, keep it locked away from the computer and always change your password when prompted. It is recommended that passwords should be a minimum of 6 characters and be a mixture of letters and numbers, i.e. using 5 instead of S, 1 instead of I, etc.
- Turn off your computer at the end of the working day.
- Never use anyone else's log on or password, even to be helpful. Never, as a manager, ask anyone to use another's password for convenience.
- Destruction and/or disposal of computer equipment must be carried out by the IT Department. This will ensure that all information is stripped from the computer and disposed of using the correct procedures. You should not remove or relocate computers without first checking with your IT Department or Systems Manager.

Printing

Staff are reminded to be vigilant when printing information, especially if the information contains:

- Patient identifiable data
- Staff identifiable data
- Commercially sensitive information

If you are printing out the type of information listed above, please ensure that you first consider whether it is actually necessary to print out the information. Ensure that you attend the relevant printer immediately so that you collect the information in a timely manner and use a pin number if possible (this depends if your local printer supports the pin system). If you come across any sensitive information unattended on a printer, remember that you need to report this as an information governance incident on the incident reporting system.

Encryption

All personal information being sent electronically e.g. on CD, USB stick, email must be encrypted.

Email encryption

Personal information should only be sent by encrypted email e.g. NHS Mail to NHS Mail because it is insecure unless encryption is available at both ends of the transmission path. If a secure route is unavailable then the information will have to be encrypted using 7 Zip free software and sent by email as an attachment.

- NHSmail encryption - The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services. If users need to exchange information securely outside of the secure email boundary they can do so by using the NHSmail encryption feature. Instruction on how to use this feature is available in the NHS Digital document Encryption Guide for NHSmail Version 2.0, October 2016 or from the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net.

Wrongly addressed

An email address that is incorrect poses a very real threat to the security of information. Messages can be addressed to the wrong person by mistake e.g. recipient with a similar name. There have been several high-profile cases of sensitive documents being sent to the wrong recipient with highly publicised consequences. Breaches of personal data must be reported in SIRMS and in some cases via the Data Protection and Security Toolkit. Serious cases must be reported to the ICO within 72 hours.

Forwarded email

The same degree of care should be taken in entering the address details when forwarding email messages to others, with removal of any recipients and/or information that is not required.

Further Advice & Assistance

There are a range of staff that can assist with difficult issues but in the first instance please contact the CSU Information Governance