NHS

Walsall Clinical Commissioning Group

Data Protection and Confidentiality Policy

Data Protection and Confidentiality Policy For Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 05 March 2019
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V1.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	05 March 2019
Date Policy is Effective From	Date of ratification
Review date:	January 2020
Expiry date:	March 2020
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff and staff working for the CCG
National Documents	
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation

Circulated to the following for consultation

Name/Committee/Group/	Designation

IG Function Leads	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author

Contents

1. Introduction

1.1 Information is a vital asset and needs to be managed securely by NHS organisation's, with effective arrangements put in place to ensure the confidentiality, security and quality of personal and other sensitive information and to ensure information is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.

1.2 In order to operate efficiently, NHS Walsall Clinical Commissioning Group (CCG) has to collect and use information about people with whom it works, including patients, public, employees (current, past and prospective), clients and customers, and suppliers. This personal information must be handled and managed appropriately, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

1.3 The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisation's. Staff working for and on behalf of the organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures. It is essential therefore, that organisation's ensure their staff understand what they need to do to keep information safe and secure.

1.4 The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) govern how data is collected, stored, processed and shared. Data Protection legislation requires every data controller who is processing personal information to notify the Information Commissioner's Office unless they are exempt. Failure to notify is a criminal offence.

1.5 The Health and Social Care (Safety and Quality) Act 2015 and the Caldicott 2 report "information to share or not to share - government response to the Caldicott review (September 2013)" have placed increased emphasis on the duty to share information between health and social care organisation's for the purposes of direct care, by professionals with a legitimate relationship with the patient.

1.6 The 6 Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS, chaired by Dame Fiona Caldicott. The Principles were extended to adult social care records in 2000.

1.7 The Caldicott2 Review Panel made a series of recommendations that were subsequently accepted by the Department of Health (DH) in a report titled "information to share or not to share - government response to the Caldicott review (September 2013)"

1.8 A 7th Principle was added. 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.

1.9 A further Caldicott Review conducted in July 2016 in a report titled "review of data security, consent and opt-outs", which made a series of recommendations in relation to ownership and responsibility for data security, implementation of effective cyber security standards, improved public awareness of information sharing and a new consent / opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care.

1.10 The GDPR (see Appendix A) was adopted by EU Member States on 25th May 2018 and includes provisions that promote accountability, transparency and governance. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Organisations are therefore expected to put into place comprehensive but proportionate governance measures such as Data Protection Impact Assessments (DPIAs), privacy by design, a record of processing activities with a view to minimising the risk of breaches, have a validated record of its processing activities and uphold the protection of personal data.

2. Purpose

2.1 The aim of this policy is to ensure Walsall CCG complies with the DPA, the GDPR, the Caldicott principles and provide a framework to enable the CCG to safeguard personal, sensitive information.

2.2 The seven principles of GDPR determine how Walsall CCG should collect, process, and retain personal data. The principles determine that we should notify the Information Commissioner of details of what data we collect and what we do with it. The principles further identify what our duties are to ensure information is kept confidential, and what our duties are to individuals in respect of their rights to see what information we hold about them.

2.2 By law, data controllers must observe these principles. Failure to do so constitutes a risk of an enforcement notification being served by the Information Commissioner and failure to comply with those notices can lead to criminal charges being brought. The principles are listed in Appendix A.

2.3 Since the processes are so similar, this policy also covers the administrative processes involved in handling subject access requests (SAR) in respect of deceased patients under the Access to Health Records Act 1990.

3. Scope

3.1 This policy applies to all CCG staff including but not limited to Governing Body members, contractors, agency & temporary staff, student, honorary and volunteer staff.

3.2 The policy applies to, but is not limited to, both paper and electronic records and the transmission of that information via fax, e-mail, post and telephone

3.3 This policy is applicable to all areas of the CCG and adherence should be included in all contracts for commissioned or collaboratively commissioned services, without exception.

3.4 This policy covers all aspects of information held within Walsall CCG, including but not limited to:

- Patient/client/service user information
- Staff information
- Walsall CCG information

3.5 This policy covers all information systems purchased, developed and managed by or on behalf of Walsall CCG.

4. Data Protection Legislation

4.1 The principles of the DPA and GDPR are based on good information handling. The principles of GDPR gives individuals' specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it (see Appendix A for further details).

4.2 GDPR came into force on 25th May 2018, with the objective of providing individuals with increased control over use of their personal data, in relation to the following principles:

- Easier access to personal data by way of a reduction in the response timeframe for all subject access requests and the removal of all associated charges.
- The right to be forgotten without the need to seek a court order
- The right to data portability between organisations in relation to personal data Implementation of "data protection by design and default" which mandates the completion of a DPIA with regard to all new or significantly changed process, policies and projects which involve the use of person identifiable information.
- Increased accountability for all organisations that process personal data demonstrated by maintaining a Record of Processing Activities which includes the technical and organisation measures taken to secure data and justification for the processing.
- Consent - It has been acknowledge that it is not always practical or appropriate for health and social care organisations to seek consent for every instance of processing personal data. As "implied consent" is not recognised under GDPR (but is still relevant in relation to the common law of confidentiality), two clear Articles have been developed which provide health and social care organisations justification to process personal data in the absence of consent. However, in order to exercise these new Articles, the organisation must document their justification for processing in their Record of Processing Activity and Fair Processing Notice.

4.3 Any person or organisation that uses personal information and determines the purpose and means of its processing is known as a Data Controller. Walsall CCG is a data controller in its own right.

4.4 Article 5(2) of GDPR requires that all data controllers shall be responsible for, and able to demonstrate compliance with the principles referenced in Appendix A.

4.5 Each organisation is required to register its data holdings with the Information Commissioner, annually, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. All applications/databases (identified in the Information Asset Register) must be registered under the CCGs global registration.

4.6 The CCG also uses other organisations to process data on its behalf such as Commissioning Support Units (CSUs), neighboring CCGs and local authorities, known as Data Processors.

4.7 Data Protection Legislation imposes certain restrictions and obligations on the data controller in relation to that processing. The data controller remains responsible for ensuring its processing complies with the DPA but the data processor does have a shared liability in their own right, and processors as well as controllers may be liable to pay damages or be subject to fines or other penalties.

4.8 GDPR restricts transfer of personal data outside of the EEA, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. The CCG maintains a Record of Processing Activities incorporating all of its information assets and maps all its data transfers in accordance with the DPA.

4.9 The Information Commissioner's Office (ICO) can issue substantial fines to organisations for failure to comply with individuals' rights or breaches of GDPR / DPA 2018.

5. Data Subject Access

5.1 The individual who is the subject of personal data is the Data Subject

5.2 The DPA gives rights to individuals to request a copy of the information held about them. This is known as a subject access request.

5.3 An individual can request access to information regardless of the media in which it may be held.

5.4 The CCG's Standard Subject Access Request Policy provides Walsall CCG with a process for the management of requests for personal information (for living individuals) under the DPA and GDPR and (for deceased individuals) the Access to Health Records Act 1990.

5.5 The CCG will ensure that the general public, staff, including volunteers, locums, temporary employees and patients are aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The CCG maintains a Fair Processing Notice on its website and statements about Data Protection will be included on all forms requesting personal identifiable information.

6. Data Protection & Confidentiality Work Programme

6.1 The key elements of the work programme are to:

- ensure compliance with all aspects of the DPA, GDPR and related provisions and provide reports to the Audit & Governance Committee
- draft and/or maintain the Data Protection policies
- promote data protection awareness throughout the organisation by organising training and providing written procedures that are widely disseminated and available to all staff
- co-ordinate the work of other staff with data protection responsibilities;
- monitor compliance with the Act and associated legislation and the effectiveness of procedures through the use of compliance checks / audits and ensure appropriate action is taken where non-compliance is identified
- maintain a Record of Processing Activities in accordance with Article 30 of the GDPR
- assist with investigations into complaints about breaches of the Act.

7. Confidentiality and Caldicott

7.1 The legal framework underpinning disclosure of confidential information includes:

- NHS Codes of Practice on Confidentiality and Information Security Management, The Caldicott Principles
- The NHS Care Record Guarantee for England
- The NHS Constitution

7.2 Caldicott 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 Access to personal confidential data should be on a strict need-to-know basis

4. Everyone with access to personal confidential data should be aware of their responsibilities

5. Comply with the law

6. Duty to share information can be as important as the duty to protect patient confidentiality.

7.3 Caldicott Guardian

7.3.1 The recommendations of the Caldicott Committee (1997 Caldicott Report) defined the confidentiality agenda for NHS organisations. A key recommendation was the appointment in each organisation of a “Guardian” of patient identifiable information to oversee the arrangements for the use and sharing of patient information

7.3.2 The Guardian should be, in order of priority:

- an existing member of the senior management team
- a senior health or social care professional
- the person with responsibility for promoting clinical governance or equivalent functions

7.3.3 The Guardian acts as the 'conscience' of an organisation, actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

7.3.4 NHS and Social Care Caldicott Guardians are required to be registered on the National Register of Caldicott Guardians.

7.3.5 The Caldicott Guardian works with guardians and SIROs in other organisation’s, for example to help manage conflicts of interest.

7.3.6 Walsall CCG staff are required to seek advice of the Caldicott Guardian on such issues and have formal sign-off in some cases; these requests are recorded in the Caldicott Log and reviewed by the Audit & Governance Committee.

7.4 NHS Care Record Guarantee

7.4.1 This sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It covers people's access to their own records; controls on others' access; how access will be monitored and policed; options people have to further limit access; access in an emergency; and what happens when someone cannot make decisions for themselves.

7.4.2 Everyone who works for the NHS, or for organisations delivering services under contract to the NHS, has to comply with this guarantee.

7.5 The NHS Constitution

7.5.1 The NHS Constitution sets out a series of patients’ rights and NHS pledges.

7.5.2 The relevant rights for this requirement are:

- You have the right to be informed about how your information is used.
- You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

7.5.3 The relevant pledges for this requirement are the NHS commits:

To anonymise the information collected during the course of your treatment and use it to support research and improve care for others. Where identifiable information has to be used, to give you the chance to object wherever possible.
To inform you of research studies in which you may be eligible to participate.

7.5.4 All NHS bodies and private and third sector providers supplying NHS services are required by law to take account of the constitution in their decisions and actions. Any breaches could have possible disciplinary sanctions or end of contract.

7.6 Common Law Obligations

7.6.1 The Common Law requires that there is a lawful basis for the use or disclosure of personal information that is held in confidence.

7.6.2 Unlike the Data Protection Act which applies to legal organisations in their entirety, the common law applies to the clinic, team or workgroup caring for an individual, i.e. those not caring for the individual cannot assume they can access confidential information about the individual in a form that identifies them even when they are working in the same organisation.

7.6.3 Normally the basis of access to confidential information will be the consent of the individual concerned and this must be obtained before disclosure or use of the information.

7.6.4 Consent can be implied in some circumstances, but not in others. It is generally accepted that consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned.

8. Using Information for Purposes Unconnected to Care

8.1 The Department of Health response to the Caldicott2 Report placed an expectation on all health and care organisations to:

- Clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes (Fair Processing Notice)
- Make clear what rights the individual has open to them, including any ability to actively dissent.

8.2 The revised NHS Constitution included a new commitment to inform people about research and to use anonymised information to support research.

8.3 Where an organisation wishes to disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

- housing departments
- education services
- voluntary services
- Police
- government departments

8.4 Individuals must also be asked for explicit consent for their confidential personal information to be shared for non-care purposes, such as those in the Table 1 below.

8.5 Where explicit consent cannot be obtained the organisation may be able to rely on the public interest justification or defence. This is where the organisation believes that the reasons for disclosure are so important that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed or for safeguarding).

8.6 The CCG complies with the Data protection legislation and where it requires identifiable data it is appropriate it will look at alternative legal basis's where there is one to process data where consent is not appropriate. This is detailed in the CCG's Fair Processing Notice.

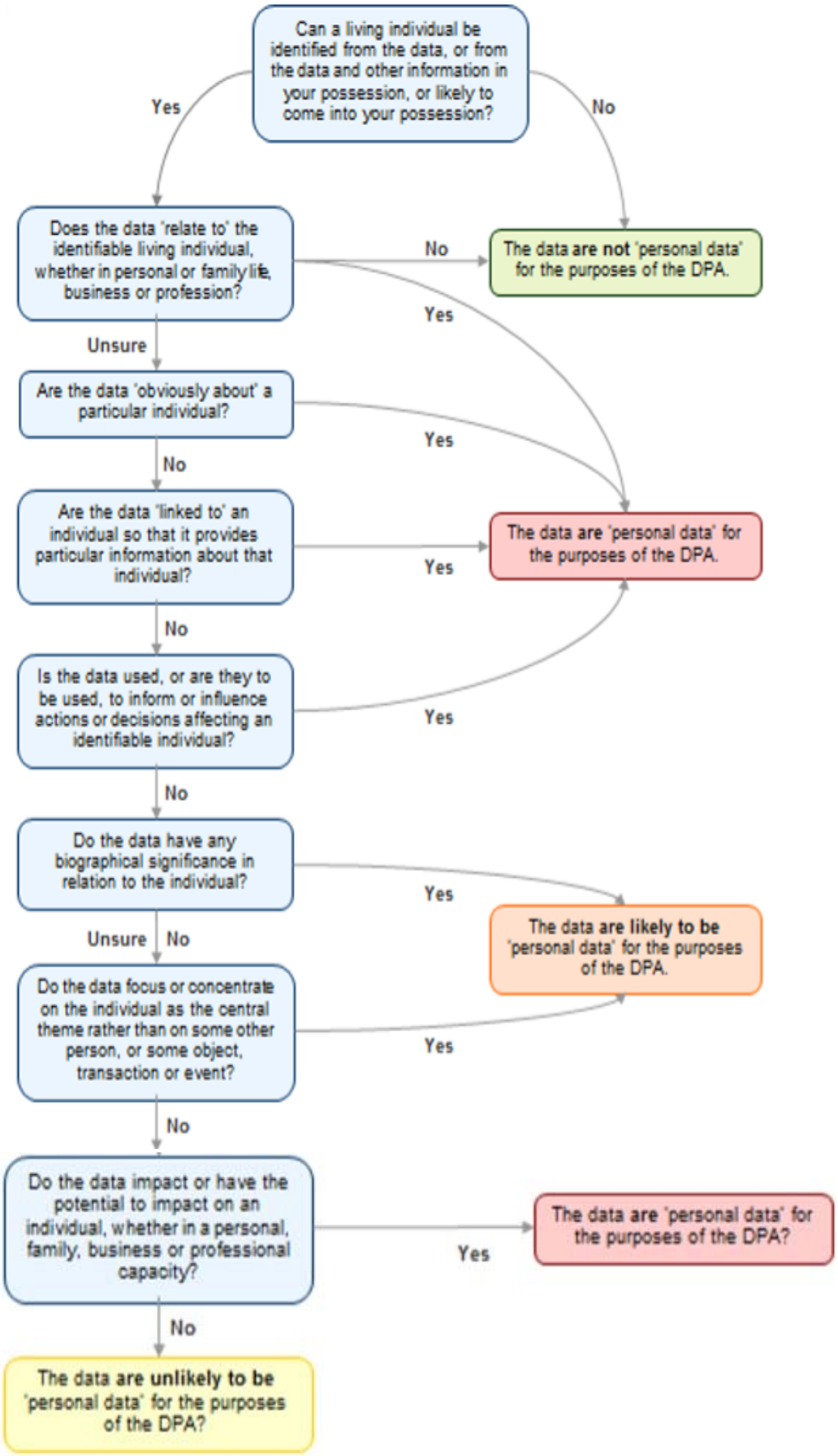
8.7 Disclosure may also be required by Court Order or under an Act of Parliament, i.e. there is a statutory or other legal basis for the disclosure. This includes disclosures permitted under section 251 of the NHS Act 2006. Applications for approval to use Section 251 powers are considered by the Confidentiality Advisory Group (CAG) of the Health Research Authority.

8.8 For any of the above disclosures the advice of the Caldicott Guardian should be sought.

8.9 Information Asset Owners (IAOs) are required to report all activities that involve the use or sharing of confidential personal information that do not have a lawful basis as a Data Security and Protection Incident, and they must be assessed in

line the ‘Guide to the Notification of Data Security and Protection Incidents’ Guidance and recorded on the organisations Data Security and Protection Toolkit where necessary.

8.10 Where the CCG contracts with a third party, the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent or some other lawful basis where required.


Can a living individual be identified from the data, or from the data and other information in your possession, or likely to come into your possession?
Yes
No
Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?
No
The data are not 'personal data' for the purposes of the DPA.
Yes
Unsure
Are the data 'obviously about' a particular individual?
Yes
No
Are the data 'linked to' an individual so that it provides particular information about that individual?
The data are 'personal data' for the purposes of the DPA.
Yes
No
Is the data used, or are they to be used, to inform or influence actions or decisions affecting an identifiable individual?
Yes
No
Do the data have any biographical significance in relation to the individual?
Yes
Unsure
No
The data are likely to be 'personal data' for the purposes of the DPA.
Do the data focus or concentrate on the individual as the central theme rather than on some other person, or some object, transaction or event?
Yes
No
Do the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?
Yes
The data are 'personal data' for the purposes of the DPA?
No
The data are unlikely to be 'personal data' for the purposes of the DPA?

9. Information Sharing

9.1 IAOs must review all their transfers of data into and out of the organisation and review the security of these transfers. The Information Asset Register will record mitigations to reduce any risk and any breaches would need to be reported to the Governance Team for recording on the CCGs IG Breach log and for review in line with the 'Guidance to the Notification of Data Security and Protection Incidents' guidance.

9.2 Decisions on whether to transfer person identifiable information must only be taken by a senior manager and/or IAO.

9.3 Of particular risk are transfers outside the UK. Under GDPR, personal data may only be transferred outside of the EEA in compliance with the conditions for transfer set out in Chapter V of the GDPR. Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

9.4 Potential risk areas to be taken into account include:

- what information is being transferred?
- have the data subjects been informed?
- to what country is the information being transferred?
- what are the purposes of the transfer?
- what data protection laws are in place in the overseas country?
- is data protection appropriately covered in the contractual arrangements between the organisations?
- is restriction on further use appropriately covered in the contractual arrangements between the organisations?
- how is the information to be transferred?
- what security measures are in place to protect the information during transfer?
- what security measures are in place in the recipient organisation?

9.5 Information about overseas transfers of information must be recorded on the CCGs Data Flow Mapping Register, included within the CCGs Data Protection notification to the Information Commissioner's Office and must also be included in the SIRO report to Governing Body, with associated risk mitigations in place to manage the risk.

9.6 The CCG will obtain an assurance statement from third parties that process the personal data of their service users or staff overseas. This assurance may be within the contract between the two organisations or within other terms of processing.

9.7 All information assets, data flows and the legal basis for sharing information will be recorded within a Record of Processing Activities in accordance with Article 30 of the GDPR.

10. Fair Processing

10.1 UK Data Protection Legislation requires that individuals are informed, in general terms, what information is collected about them, how it is held, how the information may be used the organisations or types of organisation it may be disclosed to and their rights in relation to that information. This is termed 'Fair Processing'.

10.2 Fair Processing applies equally to information about staff as it does to information about service users.

10.3 The CCG, as it does not directly provide services to service users and does not have contact with them must ensure that its website provides clear information on Fair Processing.

10.4 The CCG's Fair Processing notice must distinguish between personal information and sensitive personal information as different requirements of the DPA apply to each i.e.

- For the processing of personal information for employment purposes, it is usually sufficient to ensure that staff are aware of the types of information collected, how it will be held/stored and what the employer will use the information for, e.g. HR/personnel purposes, payroll and pensions. This is outlined within the staff Fair Processing Notice.

- For special category data, further steps need to be taken to ensure the processing satisfies one of the conditions in the Act for processing special category data. Such processing may therefore, require the consent of the employee and it is unlikely that this can be implied.

10.7 The CCG should ensure that new employees are informed (and existing employees reminded) of:

- how the organisation holds, uses and shares their personal information
- how to inform the employer of changes in their personal details
- how to raise concerns about what the organisation is doing with data that relates to them
- the method of gaining access to the records held about them (see the Management of Subject Access Requests policy)

10.8 IAOs should review all existing data collection forms to ensure that any personal information collected is actually required.

11. Roles and Responsibilities

11.1 The Accountable Officer has the ultimate responsibility for compliance with Data Protection legislation and should ensure that:

- a Data Protection Officer is appointed

- a Data Protection Lead/Manager is nominated
- the role of Caldicott Guardian is assigned and supported
- the role of SIRO is assigned and supported
- staff are made aware of individual responsibilities through policy and training

11.2 The Head of Corporate Governance supports the Caldicott Guardian and SIRO to ensure the confidentiality and data protection work programme is implemented and provides regular reports to senior management. He/she ensures the CCG adheres to the DPA and GDPR, maintaining notification, developing policies and guidance for staff and providing advice to staff.

11.3 The Data Protection Officer is responsible for informing and advise the organisation and its employees of their obligations pursuant to the GDPR and national data protection legislation, and monitoring compliance, reporting to the highest management level of the organisation – i.e. Governing Body level.

11.4 Every staff member is responsible for processing personal data, special category data and corporate data in a confidential manner, for reporting all breaches of confidentiality – both near misses and actual incidents.

12. Training

12.1 The confidentiality and data protection framework should be supported by adequate skills, knowledge and experience across the whole organisation. The levels of competency should be in line with the duties and responsibilities of particular posts to provide an adequate level of assurance.

12.2 The CCG has carried out a Training Needs Assessment (TNA) and staff are required to undertake relevant training, including mandatory Data Security and Protection training on an annual basis.

12.3 Some staff may require higher levels of awareness, specific training or a professional or other recognised qualification to enable them to carry out their duties to the level required by the organisation e.g. the necessary skills, knowledge and experience to develop corporate strategies, policies or procedures to guide staff. The CCG has outlined this in the TNA.

12.4 The TNA is monitored by the Data Protection Officer, Senior Management Team and the Audit & Governance Committee.

13. Monitoring and Assurance

13.1 The Audit & Governance Committee will review the Caldicott Log, Incident Breach log and Subject Access Requests as standing items on its agenda.

13.2 The Audit & Governance Committee formally monitors the implementation of the IG Strategy and supporting policies. It reviews the mitigation of information governance and security risks.

13.3 The SIRO will report on information risks and breaches of the Data Protection Act and Caldicott principles to the Governing Body.

13.4 The Data Protection Officer will report on the management of information assets and compliance with the CCG obligations in relation to GDPR and the national data protection legislation to the Governing Body.

13.5 There is an annual programme of internal and external audits in place which provides validation and assurance of the information governance systems.

13.6 Walsall CCG uses the complaints system to effectively respond to complaints in connection with the DPA, GDPR and Information Governance.

13.7 Training data is regularly reviewed by the Audit & Governance Committee.

13.8 Staff are expected to comply with the requirements set out within this and related policies. Compliance will be monitored via Manager and Information Governance Team reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the Data Security and Protection Toolkit.

13.9 Non-adherence to this and related policies will result in local disciplinary policies being implemented.

14. Guidance, associated legislation and References

The Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

National Information Governance Board – Applications for Section 251 Support (Integrated Research Application System – IRAS)
http://www.nigb.nhs.uk/ecc/applications-and-guidance

This has largely replaced: -

Guidance notes: Section 60 of the Health and Social Care Act 2001
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4108953

NHS Code of Practice on Confidentiality 2003 (DoH)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

The Freedom of Information Act 2000
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

The Human Rights Act 1998
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Access to Health Records Act 1990
http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

Caldicott review of Patient Identifiable Information 1997
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403

Caldicott 2 review
2013 http://caldicott2.dh.gov.uk/ (incorporating 7 Caldicott Principles)

- Common law duty of Confidentiality
- Criminal Procedures and Investigations Act 1996
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001 (Section 60)
- Registration Authority Procedures

APPENDIX A General Data Protection Regulation (GDPR) Principles

1. **Lawfulness, fairness and transparency - Article 5(1)**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. **Purpose limitation – Article 5(1)(b)**

Personal data shall be 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

3. **Data minimisation – Article 5(1)(c)**

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

4. **Accuracy – Article 5(1)(d)**

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.

5. **Storage limitation – Article 5(1)(e)**

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; 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6. **Integrity and confidentiality (security) – Article 5(1)(f)**

Personal data shall be 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.

7. **Accountability – Article 5(2)**

The controller shall be responsible for, and be able to demonstrate compliance with the other data protection principles.