NHS
Barking and Dagenham, Havering and Redbridge
Clinical Commissioning Groups

Data Protection and Confidentiality Policy

Version	Description of Change(s)	Reason for Change	Author	Date
1.0				
1.1	No Changes	Annual Review	C R Sadler	August 2014
1.2	No Changes	Annual Review	C R Sadler	November 2015
1.3	Review	Annual Review	ENW	20/12/2016
1.4	Review	Annual Review	R Meaker	23/08/2017
1.5	Updated	Policy Update	R Bada	08/10/2018
2.0	Approved	Approval	DSPG	26/10/2018

Policy Reference Number	**DSP 015**
Version Number	**1.5**
Status	**Approved**
Author/Lead	**Rob Meaker**
Implementation Date	**July 2013**
Date of Last Review Date	**20/12/2016**
Date of Next Formal Review	**August 2018**
Ratified by	**Audit and Governance Committee**
Date of Ratification	**8 January 2018**
Date of Equality Impact Assessment	**July 2013**

Contents Page

1. Introduction

Barking & Dagenham, Havering and Redbridge Clinical Commissioning Groups (BHR CCGs) has a legal obligation to comply with all legislation relevant to an individual's right of confidence and how this can be achieved and maintained in respect of data, information and IT security. BHR CCGs also has a duty to comply with guidance and codes of conduct issued by the Department of Health, NHS England, the NHS Health and Social Care Information Centre, the Information Commissioner's Office, professional bodies and other advisory groups.

This Confidentiality and Data Protection Policy details how BHR CCGs will meet its legal obligations and appropriate NHS requirements relating to confidentiality and information security standards in the use of information systems (both electronic and manual, paper-based). The requirements within the Policy are based upon the Data Protection Act (DPA) (2018), the key piece of legislation covering security and confidentiality of personal information which includes access to health records. The Access to Health Records Act (1990) applies in respect of deceased persons.

Appendix A lists associated legislation and documentation.

Appendix B summarises Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001 to make regulations to set aside the common law duty of confidentiality for medical purposes where it is not possible to use anonymised information and where seeking individual consent is not practicable. Under the Health and Social Care Act 2008, responsibility for administering these powers was transferred from the Patient Information Advisory Group to the National Information Governance Board (NIGB).

This Policy will be reviewed every 2 year's or more frequently if appropriate to take into account any changes to legislation that may occur, and/or guidance from the Department of Health, the NHS England or the Information Commissioners Office.

The Data Protection Act (2018) defines personal data as that which relates to a living individual who can be identified from that data or from that data and any other information which is in the possession of, or likely to come into the possession of the Data Controller (BHR CCGs). It also includes any expression of opinion about the individual and any intentions of the data controller or any other person in respect of the individual.

2. Scope of Policy

This policy applies to all employees carrying out work on behalf of the CCG, including Medical and Dental employees, contractors, agents, elected members, charitable groups and partners. Other service providers of the CCG should abide by their duties and responsibilities under the DPA and GDPR, which should be set out in contracts, and also taking account of any requirements within associated legislation.

To safeguard all confidential information within the CCG;

- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across the CCG;
- to ensure all staff are aware of their responsibilities with regards to confidential
- information;
- to provide all individuals working within the CCG access to the documents which set out
- the laws, codes of practice and procedures relating to confidentiality and which apply to them.

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

This policy applies to the handling of all Personal Data that is used within the CCG held on any media including Dictaphone, computer system, mobile device or manual records.

Therefore, with the exception of anonymised information, most if not all NHS information concerning patients or staff, whether held electronically or on paper, falls within the scope of the Act and therefore this Policy.

The Freedom of Information Act 2000 made a number of amendments to the Data Protection Act 1998 which widened the definition of 'data' for public bodies to cover information held in 'structured' and 'unstructured' manual records.

3. Reasons/Purposes for Processing and Data Protection Principles

The Data Protection Act requires BHR CCGs to register its data holdings with the Information Commissioners Office, identifying the purposes for holding the data, how it is processed and to whom it may be disclosed to or shared with. Failure to register or an incorrect registration is a criminal offence and may lead to the prosecution of BHR CCGs.

Processing of data is widely defined and covers all types of use including; creating, obtaining, recording, holding, altering, retrieving, destroying, disposing or disclosing of data.

The Registered Purposes apply to all those having access to information (including remote and external access) and to those engaged in duties for BHR CCGs under a contract or letter of authority, honorary contract or work experience programme; to volunteers or any other third party such as contractors, students or visitors.

BHR CCGs' reasons/purposes for processing information:

- provide health services to our patients
- maintain our accounts and records
- promote our services
- undertake research
- support and manage our employees
- We also use CCTV systems for the purpose of security and the prevention and detection of crime

There are six principles of good practice within the Data Protection Act 2018 to which BHR CCGs must adhere to all times. These are normally referred to as the 'Data Protection Principles'. Any discovered breaches of these principles should be reported as potential Information Security incidents. The Data Subject is the individual to whom the data relates:

Information as to how these principles should be applied in the course of carrying out daily duties is detailed later in this policy.

It the responsibility of BHR CCGs and its staff to comply with relevant legislation and NHS guidance, failure to do so may result in penalties being imposed upon BHR CCGs and our employees.

Six principles under DPA (2018) are listed as:

Principle 1: Lawfulness, fairness and transparency
To remain lawful, the organisation needs to have a thorough understanding of the GDPR and its rules for data collection. To remain transparent with data subjects, the organisation should state in our privacy policy the type of data we collect and the reasons for collecting it.

Principle 2: Purpose limitation

The organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

Principle 3: Data minimisation
Organisations must only process the personal data that they need to achieve its processing purposes.

Principle 4: Accuracy
The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

Principle 5: Storage limitation
The organisation need to delete personal data when it's no longer necessary.

Principle 6: Integrity and confidentiality

Personal data must 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"

4. Privacy by Design

BHR CCGs ensures that privacy and data protection matters are addressed during the design phase of any system, service product or process and is continuously addressed throughout the data lifecycle and is securely destroyed. Policies and procedures containing privacy implications are reviewed and updated on a regular basis. BHR CCGs ensures that an organisation wide approach is taken towards to data protection and privacy consideration are embedded into all processing activity it undertakes.

Data protection forms an essential part of every system and service core functionality. BHR CCGs ensures that personal data is automatically protected in every IT system, service, product and/or business practice to ensure that individuals do not have to take any specific action to protect their privacy.

5. Responsibilities and Duties

All staff have a legal duty protect the confidentiality of data and information. Day to day responsibility for enforcing the Policy and conforming to BHR CCGs registered purposes and Data Protection Principles will be devolved to Directors, Senior Responsible Information Officer, Information Asset Owners, System Managers, nominated personnel and other appropriate staff. In order to fulfil their roles, the Data Security and Protection Group or nominated officer will ensure that key messages are disseminated to staff and ensure that all staff complete mandatory IG Training. Good training, communication and awareness raising will help ensure all staff are aware of and abide by their responsibilities so as to minimise threats and vulnerabilities and ensure adequate information security and confidentiality in the process:

5.1 Accountable Officer

The Accountable Officer has overall responsibility for the Data Protection Policy within BHR CCGs which consists of:

- Overall responsibility for ensuring that the information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputation risks
- Operational responsibility for ensuring compliance with the Act will be delegated to the Operational IG Lead

5.2 The Caldicott Guardian (CG)

The Caldicott Guardian is board appointed with the strategic responsibility for overseeing the arrangements for the use and sharing of clinical information and also advises on options for lawful and ethical processing of information. The Caldicott Guardian will also play a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level. Their role is advisory and they also provide a focal point for patient confidentiality and information sharing issues. The CG acts as the 'conscience' for BHR CCGs.

5.3 Senior Information Risk Owner (SIRO)

The SIRO is an executive who leads on all matters associated with information risks and their mitigations, including information risk and methodology.

The SIRO provides the focus for the assessment and management of information risk at Board level, providing briefings and reports on matters of performance, assurance and cultural impact. The SIRO also has ultimate responsibility for providing the annual governance statement (replaces Statement of Internal Controls (SIC)) in annual reports and accounts

5.4 Data Protection Officer (DPO)

The DPO assists in monitoring internal compliance, inform and advice on the CCGs' data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact for data subjects and the supervisory authority. The DPO will report directly to the highest level of management and is given the required independence to

perform their tasks. The DPO must perform the tasks as defined in article 39 of the General Data Protection Regulation/Data Protection Act 2018.

Under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. The role of Data Protection Officer is to facilitate the CCGs compliance with GDPR and will:

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Privacy Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

5.5 IG Operational Lead

The implementation and compliance of this policy is delegated to IG Operational Lead who will support the SIRO and Caldicott Guardian.

The Operational Lead will be responsible for ensuring the data protection framework within BHR CCGs is developed, implemented and maintained, for monitoring the application of the Act and this Policy and for maintaining BHR CCGs' registration. They will providing advice and guidance on Data Protection related issues.

5.6 Data Controllers

Barking & Dagenham CCG, Havering CCG and Redbridge CCG are the overall data controller, however many people within BHR CCGs have day to day responsibility for processing data and can be seen as delegated Data Controllers. They are considered as:

- BHR CCGs' staff who alone, jointly or in common with others is responsible for ensuring that the provisions of the Data Protection Act are complied with.

Data controllers must also be aware that with increased multi-agency working and initiatives (e.g. between BHR CCGs, CSU or local authority), it may not be immediately clear to data subjects as to who the data controller actually is. Indeed, there may be more than one data controller, in which case the identity of all data controllers should be communicated to all other data subjects.

5.7 Responsible Committees

The Data Security and Protection Group is a standing committee accountable to the Audit Committee Team. Its purpose is to support and drive the broader information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation.

5.8 Information Asset Owners (IAOs)

The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets within BHR CCGs. IAOs will work closely with other IAOs of the Trust to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities, especially where information assets are shared by multiple services. IAOs will support the SIRO in their overall information risk management function as defined in Trust policy.

- What information assets are held, and for what purpose
- How information is created, amended or added to over time
- Who has access to the information and why
- Data Flows within their department inbound and outbound
- Understand and address the risk to the asset/data flows, providing assurance to the SIRO

5.9 System Managers

System Managers will be responsible for maintaining user accounts and the configuration of their nominated systems in accordance with appropriate registration and change management processes; the level of responsibility and access may vary dependant upon the system. System users should be informed as to the appropriate systems manager for their application.

6.0 Information Asset Administrators

The Information Asset Administrator's (IAA) primary role is to support the IAO to fulfil their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

- Ensure that policies and procedures are followed
- Recognise potential of security incidents and report all actual occurrences and near misses
- Consult their Information Asset Owner on incident management
- Ensure that any information asset registers are kept accurate and up to date.

These will be identified by the IAOs.

6.1 Individual Responsibilities

All staff will be responsible for effective information governance including (but not limited to):

- Discharging of their legal, ethical and contractual responsibilities for processing information regardless of their position (whether directly employed or not), standing or level of knowledge. This includes permanent, temporary, locums, voluntary, work experience and bank staff, including contractors and partners involved in the organisation business related activities
- Abiding by legislations, professional standards, codes of conduct, policies and any locally agreed standards
- To report immediately any actual or potential threats that may be encountered in relation to Information Governance /Security

- To ensure full compliance to this policy and all other Information Governance related documentation that may be issued throughout the organisations'.
- To ensure that any relevant, mandatory Information Governance training is completed annually. Staff who has taken on additional responsibilities must ensure that they complete any additional relevant IG training in order to equip them with the skills and knowledge to perform their duties to a continual high standard.
- At all times to strive to achieve best practice standards with full compliance towards professional codes of conduct. For further information please visit:

  www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/lglobligat.pdf

All staff and patients have the right to request from the organisation what personal data is held about them on the organisation records.

6. The Right of Subject Access

In general the Act gives data subject the rights to access personal data about themselves which is held in either electronic or manual form, whenever the record was compiled. The right give entitlement to:

- Be informed whether personal data is processed
- A description of the data held, the purposes for which it is processed and to whom the data may be disclosed
- A copy of the information constituting the data
- Information as to the source of the data

It is the responsibility of Caldicott Guardian to develop and maintain procedures relating to Subject Access requests for Service Users.

The DPA (2018) does not state specifically how a valid request can be made, therefore an individual has the option to make a subject request to any part of BHR CCGs either verbally or in writing (also via social media) and does not have to be to a specific person or contact point.

As long as it has been made clear that an individual is asking for their own personal data, they are not obliged to use the phrase of 'subject access request' or Article 15 of the DPA (2018).

The Caldicott Guardian must gain sufficient assurances that the request comes from the Data Subject or their representative.

The DPA (2018) requires organisations to act on the subject request without undue delay and at the latest within 28 days of receipt.

The time limit should be calculated from the day after the subject access request is received (whether the day after is a working day or not) until 28 days later.

Both BHR CCGs and any partner organisations will require arrangements for any joint records held. It will be the responsibility of the Caldicott Guardian to ensure that such arrangements are up to date and information disseminated accordingly.

The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased patients' records.

6.1.1 The Right to Prevent Processing Likely To Cause Harm or Distress

BHR CCGs are exempt from processing data which will or are likely to cause the data subject or another person unwarranted and substantial harm or distress.

This restriction does not apply if you are satisfied that the health data has already been seen by, or is known by, the individual it is about.

Any requests not to process data should be referred to the Caldicott Guardian for consideration.

6.1.2 The Right to Prevent Unsolicited or Direct Marketing

An individual can ask the organisation to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for the organisation to refuse. Therefore, when the organisation receive an objection to processing for direct marketing, the organisation must stop processing the individual's data for this purpose.

6.1.3 The Right to Prevent Automated Decision Making

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

6.1.4 The Right to Claim Compensation

Individuals have a right to seek compensation from the data controller for damage or distress caused by any contravention by a Data Controller under the requirements of the Data Protection Act 2018.

6.1.1 The Right to Rectification, Blocking, Erasure and Destruction

Under Article 16 of the DPA (2018) it provides rights to individuals to have their inaccurate personal data rectified or completed if it is incomplete (depending on the purposes for the processing). This request for rectification can be made verbally or in writing. A respond to the request must also be issued one month from receiving the request, however, there are circumstance in which a refusal for rectification may be granted.

The importance of how accurate the personal data should be, should dictate the efforts that should be put in ensuring the data is accurate.

Staff must satisfy themselves that the person requesting the correction is the Data Subject (or their formal representative).

Depending on the nature of the request and the data in question, requests may be referred to the Caldicott Guardian who should ensure that procedures are in place to manage the process and that guidance is available to all staff who manage data.

Patients do have the right, under the Data Protection Act, to ask for factual inaccuracies in the record to be rectified or deleted. The Act does not, however, give them the right to ask for entries expressing professional opinions to be changed. You should only comply with a request if you are satisfied that it is valid – e.g. the entry is indeed factually inaccurate, but if you decide that a correction is not warranted, you should still annotate the disputed entry with the patient's view.

6.1.5 The Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Data Subjects have the right to request the Information Commissioner for an assessment if they believe that the Trust is not complying with the requirements of the Data Protection legislation.

7. Enforcement Notices

The Information Commissioner has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. It is important to note that these powers are focused on ensuring that organisations meet the obligations of the Act.

All portable devices (for example laptops), prior to use must be encrypted in accordance with BHR CCGs policy and procedures.

Measures should be taken to ensure that all software and data is always removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from BHR CCGs or its contracted ICT service provider.

Manual records containing person identifiable or confidential information (only after a review has taken place by the Caldicott Guardian where it has been established that the information can be destroyed) should either be shredded or disposed of via shredding or confidential waste bins/sacks which should be collected and held in a secure area prior to disposal in accordance with BHR CCGs waste disposal processes.

7.1.2 Back-ups

As stated above, any electronic person identifiable or confidential data must be stored on BHR CCGs or its contracted service provider's allocated and controlled network drives. It is the responsibility of BHR CCGs or its contracted Service Provider to manage backups in accordance with defined backup procedures.

7.1.3 Transfer of Information/Information in transit

If person identifiable information or any held medical records need to be transported then strict security and confidentiality of such information should be maintained at all times to ensure that the information is not subject to compromise during transit. This will apply to both manual records and electronic records contained on any media.

Royal Mail recorded delivery / courier service should be used at all times. A record must be kept of what information has been sent, by whom to whom, detailing method of transportation used (this should also be signed and dated). Packaging must be carefully considered and must be sufficient to protect the contents from any physical damage during transit.

Contracts between BHR CCGs and third parties should include appropriate confidentiality clauses which should be disseminated (and signed and dated) to the third parties employees.

Emailing of data should only be undertaken between secure, encrypted email services such as NHS. Mail. Emailing outside of these is not accepted. (E.g. NHS generic-mail accounts to Outlook or vice versa).

Safe Havens should be carefully considered and established for the sending and receiving of confidential faxes with relation to PID (or other sensitive or confidential information) in accordance with BHR CCGs Information Security Policy.

8. Training

The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA / GDPR and their IG obligations and this will be carried out by regular mandatory Information Governance training sessions. Any new staff members (including temporary, contractors) will be required to complete Information Governance as part of their induction.

Information Governance training is required to be undertaken by all CCG employees and those providing a service to the CCG. All NHS staff are mandated to undertake annual Information Governance training.

Where staff have specific Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO etc. additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the Information Governance Training Needs and Analysis (TNA) document.

To maintain high staff awareness the CCG will direct staff to a number of sources:

- Policy/strategy and procedure;
- Manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff Intranet.

9. Contracts of Employment

Staff contracts of employment (whether legacy PCT or new Organisation's contracts) must include appropriate clauses relating to data protection and confidentiality.

Appropriate clauses must also be included in any contracts for 3rd party providers.

If no formal contract exists, e.g for volunteers or students then the individual must sign to confirm that they agree to abide by the same conditions.

Staff contracts must also include a clause confirming the individual has provided the necessary authorisation for BHR CCGs to process and retain their information as part of their contract of employment. This also gives staff the right to request access to their HR records.

10. Disciplinary

A breach of the Data Protection requirements could result in a member of staff facing disciplinary action up to and including dismissal.

11. Monitoring & Audit

The Data Security and Protection Group or responsible officer will oversee the implementation and day to day management of this policy.

This policy and associated appendices and procedures will be monitored by the DSPG who are responsible for maintaining its currency and relevance.

It is also assumed that both Internal and External Audit will review this and associated policies and procedures. Findings of these audits and reports of progress against any action plans will be made to Data Security and Protection Group and the Audit and Governance Committee.

Regular audits of quality, completeness of data held on computerised systems to ensure compliance with the Data Protection Principles may be undertaken at any time. The results of these audits will be reported to the Data Security and Protection Group along with actions for improvement identified and members assigned to complete actions within an agreed timeframe.

All serious incidents as defined in the Serious Incidents Requiring Investigation (SIRIs) will be notified to the IG Lead/ Data Protection Officer and be investigated thoroughly and reported to The ICO, NHS England and The Department of Health.

12. Review

This policy will be subject to a 3 year review unless legislation or practice necessitates otherwise.

Appendix A

Associated Documentation

This Policy should be read in conjunction with the following:

Legislation to restrict disclosure of personal identifiable information

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

Legislation requiring disclosure of personal identifiable information

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Other Relevant Acts of Parliament

Human Rights Act 1998

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Acute Trusts, Organisation's and individual doctors, dentists, pharmacists treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority 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, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take individuals rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act was introduced in November 2000 and became enforced from the 1st January 2005. The Information Commissioner (previously the Data Protection Commissioner) oversees the implementation of this Act and ensure regulation. This Act gives individuals rights of access to certain held and recorded information held by public authorities subject to certain

exemptions and conditions. The main aim of the Act is to provide transparency in how NHS organisations operate, make decisions and spend money.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with BHR CCGs holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. The CCGs will issue each user an individual user-id and password which will only be known by the individual and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

The CCGs will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records Act 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 2018.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Overview of Legislation & NHS Guidance

Health Service Guidance (HSG)
HSG (96)15 The NHS Information Management & Technology Security Manual

E5498 Ensuring Security & Confidentiality in NHS Organisations;

Provides detailed instructions for NHS bodies to comply with security requirements to protect an individual's confidentiality and the security of information systems.

HSG (96)18 The Protection & Use of Patient Information

Gives NHS bodies guidance concerning the uses and protection necessary for patient information. It also considers ways of obtaining and using patient information to comply with Data Protection legislation, current and planned.

HSC 1999/012 Caldicott Guardians HSC 2002/003

Caldicott Guardians & Implementing the Caldicott Standard into Social Care

British Standards BS7799 Information Security Standards

This is the accepted industry standard for Information Management and Security. This standard has been adopted by BHR CCGs all NHS organisations now have to ensure compliance with these requirements. It is also a recommended legal requirement under the registration and principle 7 of the Data Protection Act.

All NHS organisations have been sent a copy of the BS7799 GAP analysis software by the NHS Information Authority to assist with the process of compliance with the BS7799 standard.

Department of Health Records Management: NHS Code of Practice (Part 1 and Part 2)

A guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

The Code provides a key component of information governance arrangements for the NHS. The guidelines apply to NHS records of all types regardless of the media on which they are held. They may consist of patient health records, administrative records, e-mails, audio and video tapes, CD-ROM etc.

Appendix B

Section 251(s.251)

13. Section 251 of the NHS Act 2006

Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001. The terms Section 60 and Section 251, when used in relation to use of patient information therefore refers to the same powers. These powers allow the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for medical purposes where it is not possible to use anonymised information and where seeking individual consent is not practicable. Under the Health and Social Care Act 2008, responsibility for administering these powers was transferred from the Patient Information Advisory Group to the National Information Governance Board (NIGB).

14. Why was Section 251 created?

Section 251 came about because it was recognised that there were essential activities of the NHS, and important medical research, that required use of identifiable patient information but because patient consent had not been obtained to use people's personal and confidential information for these other purposes, there was no secure basis in law for these uses. [NB. There are a few exceptions where there is a legal basis for disclosure e.g. reporting of notifiable diseases]. Section 251 was established to provide a secure legal basis for disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent was not practicable, having regard to the cost and technology available.

It was anticipated when Section 251 powers were originally established that the NHS would develop mechanisms to seek, record and implement consent. Also that the NHS would endeavour to improve data quality and develop processes to link data in pseudonymised form, reducing the need for identifiable data to be used. These mechanisms are still being developed. It has since been acknowledged that there will continue to be a need for Section 251 powers, for some uses, on a more long-term basis.

15. How is Section 251 administered?

The Health Service (Control of Patient Information) Regulations 2002 (SI 1438) were made under Section 60 of the Health and Social Care Act 2001 and continue to have effect under Section 251 of the NHS Act 2006. These regulations established a class support mechanism whereby Section 251 powers could be used by the Secretary of State without needing to lay regulations before Parliament for each use of the powers. The classes of support are:

- To reduce the identifiability of data.
- For the past or present geographical location of patients for medical research.
- To identify and contact patients with a view to inviting them to participate in medical research or to allow their data or tissue to be used for medical research or to allow their tissue to be used for other medical purposes.
- To link information from more than one source or to validate the quality and completeness of confidential patient information or information derived from patient data.
- For the audit, monitoring and analysing of the provision made by the health service for patient care and treatment.

- To allow access to confidential patient information for one or more of the above purposes.

[Paraphrased from Schedule 1 of the 2002 Regulations]

Additionally, these regulations provided specific support under Section 251 for the Health Protection Agency and other public health staff to collect data relating to communicable disease surveillance and for surveillance of other risks to public health. They also provided specific support for Cancer Registries to collect data relating to cancer.

The National Information Governance Board and its Ethics and Confidentiality Committee do not have statutorily delegated authority from the Secretary of State but rather advise the Secretary of State on the use of Section 251 powers and make recommendations about applications for approval under Section 251. The NIGB has agreed to delegate its responsibility for administering Section 251 powers to its Ethics and Confidentiality Committee.

As and when the above regulations need revision, Section 251 requires that the Secretary of State consults the NIGB prior to revised regulations being laid before Parliament.

Appendix C

Glossary

Term	Definition
Organisation	**Refers to BHR Clinical Commissioning Groups**
DPA	**Data Protection Act**
GDPR	**General Data Protection Act**
HSG	**Health Service Guidance**
IAA	**Information Asset Administrator**
IAO	**Information Asset Owner**
ICO	**Information Commissioners Office**
NIGB	**National Information Governance Board**
PID	**Person Identifiable Data**
SIRO	**Senior Information Risk Owner**
SIC	**Statement of Internal Control**
SIRI	**Serious Incidents Requiring Investigation**

Appendix D- Equality Impact Assessment Tool

Equality Impact Assessment Form		
Policy author: Rob Meaker (Executive Lead)	Date of assessment: September 2013	
Title of policy: Information Governance Policy	Is this a new or existing policy? EXISTING	
1. Is there a concern that the policy does or could have a differential impact in any of the following areas?		
	Y/N – delete as appropriate	
Age	Yes	No **X**
Civil partnership/marriage	Yes	No **X**
Disability	Yes	No **X**
Faith or religious beliefs	Yes	No **X**
Gender	Yes	No **X**
Race	Yes	No **X**
Pregnancy/maternity	Yes	No **X**
Sexual orientation	Yes	No **X**
Transgender	Yes	No **X**
2. If the answer is 'no' for the groups above, please sign and date the form and add this form to the end of the policy. 3. If the answer is 'yes' for any of the groups above, please explain the reasons and complete box 4 (below). For help please contact the engagement adviser for advice (020 8926 5048).		
4. Are there any additions or actions to be added to the policy which ensure the policy does not have an adverse impact on any of the protected groups? If the answer is "yes", please detail below.		
Signed: Rob Meaker (Executive Lead)		**Date:**
Your contact details (department; e-mail; telephone number)		rob.meaker@nhs.net