NHS
Bradford District and Craven
Clinical Commissioning Group

CONFIDENTIALITY AND DATA PROTECTION POLICY (Incorporating Information security)

This policy provides a guide to the key elements of the legal framework governing information handling; outlines the responsibilities in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

Key information

Responsible director:	IG Lead, Sue Baxter
Author:	IG Officer, The Health Informatics Service (THIS)
Approval body:	Records Management Group (RMG)
Date approved:	March 2021
Version:	1.0
Review date:	March 2023

Version control

Version no.	Date	Author	Description	Circulation
0.1	June 2020	As above	Draft Confidentiality and Data Protection Policy	Head of Governance
0.2	September 2020	As above	Review of IT sections	Associate Director of Digital Senior Primary Care Senior IT Business Manager
0.3	September 2020	As above	THIS DPO review	Data Protection Officer (THIS)
0.4	September 2020	As above	Final review	Strategic Head of Assurance
0.5	July 2021	As	Review	IG Officer – THIS

Version no.	Date	Author	Description	Circulation
		above		
1.0	March 2021	As above	Approved	Audit and Governance

Contents

Key information 1

Version control 1

1 Introduction 5

2 Scope of the policy 5

3 Associated documentation 6

4 Policy statement 7

5 Aims and objectives 7

6 Definitions / explanation of terms 7

7 Duties, accountabilities, roles and responsibilities 7

7.1. Duties within the organisation 7

7.2. Responsibilities for approval 7

8 Policy and procedure details 8

8.1 Personal confidential data……8

8.2 Sensitive personal data……8

8.3 Direct and indirect care……8

8.4 Consent……9

8.5 Corporate information……9

8.6 Data controller……10

8.7 Data processor……10

9 Confidentiality, guidance and legislation……10

9.1 What is the UK data protection law now the brexit transaction period has ended…..10

9.1.1 Individuals rights under GDPR……11

9.2 Data protection act 2018……11

9.3 Human rights act 1998……11

9.4 Common law duty of confidentiality……12

9.5 Caldicott principles……12

10 Ensuring informationis secure and confidential……12

10.1 General principles……12

10.2 Using and disclosing confidential patient information for healthcare purposes……13

10.3 Using and disclosing confidential staff information …..…….13
10.4 Using and disclosing corporate and business information…..…….13
10.5 Information security……..13
10.5.1 Information security procedures…….13
10.5.2 Passwords……..14
10.5.3 National applications systems controls……..14
10.5.4 Information technology (IT) access controls ……...14
10.5.5 Connection to the CCG network..…… .15
10.5.6 Remote working……..…….15
10.5.7 Portable devices……..…….15
10.5.8 Unsupported systems, software and updates…….15
10.5.9 New and changed IT systems……18
10.6 Sharing personal confidential information without consent ……..18
10.6.1 National Data Opt Out…….19
10.7 Confidentiality and conversations…….19
10.8 Records management ……..19
10.9 Access to records……..……..19
10.10 Information sharing…..…….19
10.11 Information confidentiality incidents.……20
10.12 Data protection impact assessment…….……..20
11 Dissemination, implementation and training 21
12 Review and monitoring..... 21
13 Public sector equality duty..... 21
14 Consultation 22
15 References..... 22
16 Appendices 23

1 Introduction

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

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

2 Scope of the policy

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, Clinical Board, Clinical Executive, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCG. The policy is applicable to all areas of the organisations and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

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

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

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

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

Confidentiality and data protection within an independent contractor's (such as GPs and dentists) premises is the responsibility of the data controller (owner/partners). However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

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

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

3 Associated documentation

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

- Abortion Regulations 1991
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998 (as amended by the Criminal Justice and Immigration Act 2008 and the Legal Aid, Sentencing and Punishment of Offenders Act 2012)
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- National Data Guardian report
- Health and Social Care Act 2018
- Human Fertilisation and Embryology Act 2008
- NHS Sexually transmitted disease regulations 2000
- Terrorism Act 2006
- Privacy and Electronic Communications (Amendment) Regulations 2018
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 2013
- Public Records Act 1967
- Regulation of Investigatory Powers Act 2000 (and Interception by Businesses etc. for Monitoring and Record-keeping purposes Regulations 2018)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act (Amendment)1992
- The Children Act 1989 and 2004 (and The Children and Young Person Act 2008)

Networks and Information Systems (NIS) Directive

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

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

4. Policy statement

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

5 Aims and objectives

The CCG has established, implemented and maintained procedures linked to this policy to ensure compliance with the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), Data Protection Act 2018 (DPA) and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit.

This policy supports the CCG in its role as a commissioner of health services and will assist in the safe sharing of information with its partners and agencies.

6 Definitions / explanation of terms

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

7 Duties, accountabilities, roles and responsibilities

7.1. Duties within the organisation

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

- Governing Body
- Audit and Governance Committee
- Accountable Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Data Protection Officer
- IG Lead (Strategic Head of Assurance)
- Associate Director of Digital and Technology
- Information Asset Owner
- Information Asset Administrator
- Heads of service
- All employees

7.2. Responsibilities for approval

The Records Management Group are responsible for the approval of this policy document. The accountability and responsibility are set out in more detail in the Information Governance Framework which must be read in conjunction with this policy.

8 Policy and procedure details

8.1 Personal Confidential Data

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

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

8.2 Sensitive Personal Data

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

- Physical and mental health
- Genetic data
- Biometric data
- Social care
- Ethnicity and race
- Sexuality
- Trade union membership
- Political affiliations
- Religion
- Records relating to criminal charges and offences

8.3 Direct and Indirect care

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

Direct care

"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care"

The NHS is trusted to collect, store and safeguard data and people expect information to be used for direct care.

Indirect care

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

The CCG adheres to national guidance in relation to using personal confidential data for commissioning purposes and recognise that such data can only flow where a clear legal basis enables this.

Those individuals who decide that they do not want their information to be used for these activities should be able to stop access to her or his data for such activities.

8.4 Consent

The General Data Protection Regulation is very clear when it comes to organisations sharing an individual's information with another organisation that this consent must be for a specific purpose, the individual must fully informed of that purpose, which must be unambiguous and consent must be freely given by the individual. Their information must not be further processed for purposes that are incompatible with these purposes.

It is also required that consent obtained is recorded for each information sharing purpose and that this is fully auditable.

However, consent may not be the preferred legal basis for the processing of personal data for GDPR purposes.

The likely legal bases (others are available) for processing most health and social care data are:

- For processing personal data - **Article 6(1)(e)** - Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For processing special categories of personal data - **Article 9(2)(h)** (and DPA) - Necessary for the purposes of health or social care (which includes the management of health or social care systems and services).

More information is provided within the CCG Privacy Notice, available from the organisation's website.

8.5 Corporate information

Corporate information includes:

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

Corporate information could be accessible through the Freedom of Information Act either from the CCG responding to a request for information or through making information accessible via the CCG's Freedom of Information Publication Scheme (available on the CCG's website).

Where any corporate information has a duty of confidence attached to it, the information may be exempt from release. Additionally, other exemptions of the Act could restrict release of certain corporate information.

8.6 Data Controller

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

8.7 Data Processor

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

9 Confidentiality, guidance and legislation

For personal and confidential information held by the CCG there will be appropriate measures to ensure confidentiality and security, in accordance with the National Data Guardian standards, NHS Digital Guidance, Information Commissioners Office (ICO) and professional Codes of Practice, legislation and common law.

9.1 What is the UK data protection law now the Brexit transition period has ended?

The Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context. The principles of the EU GDPR have been incorporated in UK Data Protection law to reflect that the Brexit transition period has ended.

The ICO will remain the independent supervisory body regarding the UK's data protection legislation. The UK government will continue to work towards maintaining close working relationships between the ICO and other countries' supervisory authorities.

It is important to note that:

- a personal data breach' is defined in the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed"
- all actual information breaches must be reported (to the ICO) via the Data Security and Protection Toolkit within 72 hours of becoming known by the data controller.
- data processors must report the incidents to the data controller without undue delay after becoming aware of it; data processors can be held liable for breaches.
- the penalty for breach of the regulations is now capped at a maximum of £17 Million (€20,000,000) or 4% of the turnover of an organisation
- organisations must employ the 'privacy by design' approach to activities involving personal data; a Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high

privacy risk

- privacy information notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulation if their customers/clients are based within the EU
- the consent and opt-out model for processing personal data is in process of being further defined (see Caldicott 3 report and corresponding consultation and direction from the Department of Health)
- a register of data controllers is maintained by the ICO and organisations and require fee paying organisations to complete/renew an annual submission
- data subjects have the new right to erasure, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within one month of data of receipt of the request and provided free of charge (unless a request is "manifestly unfounded or excessive")

9.1.1 Individuals rights under GDPR

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

These rights are not absolute: for example, the right to erasure (also known as 'the right to be forgotten') does not apply to health or social care records.

Requests from individuals wishing to exercise any of their rights under GDPR/DPA should be referred to the Head of Corporate Governance first instance.

9.2 Data Protection Act 2018

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

The Act is enforced by the ICO. Fines can be made against organisations or persons holding personal information (data controllers) of up to £17 Million (€20,000,000) or 4% of the turnover of an organisation where there is a serious breach of the Act e.g. loss of personal data of many individuals.

9.3 Human Rights Act 1998

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

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

9.4 Common Law Duty of Confidentiality

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

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

9.5 Caldicott Principles

Dame Fiona Caldicott produced an initial report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure.

The Caldicott Guardian has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. A detailed description of the Caldicott Function is given in the Information Governance Strategy.

The recommendations of two further reports by Dame Fiona have been largely accepted by the government, resulting in:

- a revised set of Caldicott Principles (2020) which should be observed when using or sharing patient information (See Appendix C) and
- Ten Data Security Standards (2017) which now form the basis for information governance across the health and care sector (See Appendix B).

10. Ensuring information is secure and confidential

10.1 General principles

- The CCG regards all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCG have established and maintained policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality and the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, via the Data Protection Impact Assessment (DPIA), Information Asset Register (IAR) and Data Flow Mapping (DFM) processes will be undertaken in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable confidentiality and data protection controls are in

place.

Where any disclosure of PCD is made there a must be a legal basis for doing so.

10.2 Using and disclosing confidential patient information for healthcare purposes

- The use and disclosure of their healthcare information and records.
- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.
- The potential use of their records for the clinical governance and audit of the care they have received.
- Through a privacy notice outlining what information will be shared, the purpose of this, who the data will be shared with, how long data will be retained, the rights of the data subject (including opt-outs) and what security measures are in place to protect confidentiality.

10.3 Using and disclosing confidential staff information

Similarly, GDPR recognises 'legitimate interests' as the lawful basis for most information sharing for employment purposes, for example communications related to an employee's role, salary payment and pension arrangements. Staff should be made aware of the ways in which their information is used, and that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of Freedom of Information requested where the public interest in disclosure is deemed to override confidentiality considerations. The CCG include this within their privacy notice for staff in respect of how their information is processed.

The consent of staff members must be sought where the processing is not *necessary* for routine employment purposes, for example when referring a member of staff to Occupational Health Services.

10.4 Using and disclosing corporate and business information

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

Corporate information could be accessible through the Freedom of Information Act either from the CCG responding to a request for information or through making information accessible via the CCG's Freedom of Information Publication Scheme.

10.5 Information security

10.5.1 Information security procedures

The security of paper and electronic records, computers and networks is controlled by policies and procedures that have been authorised by the appropriate authority within the CCG, or IT service provider where the asset is provided under contract to, or managed on behalf of, the CCG.

Areas of information security covered by this policy include, but are not limited to:

Location Access Controls

- Only authorised personnel who have an identified need will be given access to restricted areas containing information systems such as a server room or a filing room.

User Access Controls

- Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager or sponsor.
- Access to electronic information systems is given at the appropriate level for the agreed need.
- When previously granted permissions are no longer required by an individual due to changes in job roles or services, such permissions must be revoked. Arranging for this to occur is the responsibility of line managers.
- Dormant or unused accounts will be disabled and deleted when identified.

10.5.2 Passwords

The primary form of access control for the CCG's computer systems is via password. Each member of staff using a computer system will have an individual password.

Sharing of passwords by both the person who shared the password and the person who uses it is an offence under the Computer Misuse Act 1990. All staff must follow robust security practices in the selection and use of passwords. Logon details are not to be shared or used under supervision even in training situations.

Detailed password guidelines are attached at **Appendix D** of this policy.

10.5.3 National Applications Systems Controls

National spine enabled systems are protected by a number of different security

mechanisms including:

- Smartcard: Access will be restricted through use of an NHS Smartcard with a pass code, provided by the local Registration Authority
- Training*:* Access to the NHS Care Record Service will only be allowed following Data Security Awareness training
- Legitimate relationships*:* Staff will only be able to access a patient's record if they are involved in that patient's care
- Position Based Access Control (PBAC)*:* Access will depend on staff roles/job/position functions. Roles and access privileges will be defined centrally and given locally by people designated to do this in the organisation
- Sealed envelopes: Patients will be able to hide certain pieces of information from normal view. This will be called a patient's sealed envelope
- Audit trails*:* Every time someone accesses a patient's record, a note will be made automatically of who, when and what they did
- Alerts*:* Alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs e.g. if breach of sealed envelope, or no legitimate relationship being present

10.5.4 Information Technology (IT) Access Controls

- Access to IT equipment, for example, PCs and terminals is restricted to

authorised users who have an agreed requirement to use those facilities

10.5.5 Connection to the CCG Network

- All devices connected to the CCG's network are governed by the IG Statement of Compliance provided to NHS Digital.
- The connection of any equipment to the CCG's network requires authorisation from IT services.
- All electronic processing devices connecting to the CCG's network must have regularly updated operating systems and software and be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that all software, including the anti-virus protection, is up to date.
- Personally owned devices should only be directly connected to the network with appropriate authorisation. Personally owned means devices that are not provided by the CCG, IT service provider or another NHS organisation and directly connected means either by wire (network cable) or W
- Wi-Fi. External visitors may connect to the internet via a Guest Wi-Fi account.

10.5.6 Remote Working

- Information that is taken off site must be authorised by line management, protected by adequate security and, where held on portable computers, backed up regularly to the CCG's server. Portable devices must be used in line with CCG procedures and protected by appropriate security.

Working from home must be authorised by line management and comply with policies relating to information governance.

10.5.7 Portable Devices

- The use of portable devices for work purposes must be in line with CCG policy and authorised by your line manager (and information governance/IT services where appropriate).
- Only portable devices that have been provided / authorised for use by IT Services may be used for work purposes. This includes, but is not limited to, laptops, tablets such as iPads, USB sticks, digital dictation machines, smart phones.
- Personally owned portable devices such as laptops and iPads must not be directly connected to the network either by wire (network cable) or Wi-Fi without authorisation.
- Portable storage devices (including CDs, DVDs and flash drives) containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on CCG equipment and must be protected by proper security (ask IT Service Desk for advice).
- Portable devices such as laptops, tablets (for example, iPads), dictation machines smart phones and USB sticks must be encrypted and, where appropriate, have up to date antivirus software.

Portable devices used to access NHSmail must be encrypted and have the capacity, and be configured, to allow remote wiping.

10.5.8 Unsupported Systems, Software and Updates

- The CCG will use countermeasures and management procedures to protect itself against the effects of malicious software. All staff are expected to co-

operate fully with this requirement.

- No unsupported, or out of warranty systems; operating systems; software or applications shall be used for CCG business without permission of the SIRO.

All operating systems and applications used for CCG business must be kept up to date using available and appropriate software updates.

Monitoring System Access and Use

Audit trails of system access and use are maintained and should be reviewed on a regular basis. They will also be used to investigate any potential concerns that require further investigation.

The CCG reserves the right to monitor access where it suspects there has been a breach of policy. Measures to limit suspicious logons and excessive or adverse systems use may be implemented.

In exceptional circumstances an investigation under the powers granted by the Regulation of Investigatory Powers Act 2000 may be considered.

Business Continuity

The CCG will ensure that business continuity and disaster recovery plans are produced, with support from its IT service provider, for all critical information, applications, systems and networks.

Reporting Security Incidents and Weaknesses

- All information management and technology security incidents and weaknesses must be reported via CCG incident reporting procedures (complete an IR1 form and send to the Corporate Governance team; the IR1 form can be found here: M:\Data\Core Docs\Templates
- Incidents that present an immediate risk to the CCG such as viruses should be reported to the IT Help Desk immediately.
- All security incidents investigated and resulting in an actual or potential breach of confidentiality must be reported in accordance with incident reporting policies and procedures including notification to the SIRO or Caldicott Guardian as appropriate.
- All employees must promptly report any information governance incidents or near misses to the Governance team in line with the CCG's Incident Reporting Policy (available on the CCG Intranet). A sufficiently serious information governance breach must be reported to the Information Commissioners' Office within 72 hours of the breach being identified, it is therefore vital that any information governance incidents are reported promptly.
- The Information Asset Owner should conduct risk assessments following any incident to ensure any risks are effectively managed.

Risk assessments

The CCG in conjunction with its IT service provider will carry out security risk assessments in relation to all the business processes covered by this policy. These risk assessments will cover all information systems, applications and networks that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability. Once identified, information security risks shall

be managed on a formal basis. Where appropriate, they shall be recorded within the CCG's risk register and action plans shall be put in place to effectively manage those risks.

10.5.9 New and changed IT systems

Project manager responsibilities

Project managers are responsible for ensuring the production and implementation of effective security countermeasures and relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the System Level Security Policies and Privacy Impact Assessments, as part of the project to implement a system.

System change control

The CCG will ensure that the relevant project managers or Information Asset Owners (IAOs) will review changes to the security of any information system, application or network. In addition they should consult with the CCG's IT service provider prior to all such changes being made. The relevant project manager or IAO is responsible for updating all relevant system documentation.

The IAO may require checks on or an assessment of the actual implementation based on changes implemented.

Technical compliance checking

The SIRO will seek assurance from the IT service provider that information systems are regularly checked for compliance with security implementation standards.

Transfers of confidential or sensitive data

Any non-routine bulk extracts (21+ records) or transfers of particularly confidential or sensitive data must be authorised by the responsible manager or the Information Asset Owner for the work area and may require approval by the SIRO. See Records Management Policy for further guidance.

Secure disposal or re-use of equipment

All staff must ensure that where equipment is being disposed of or re-issued, all data on the equipment (e.g. on hard disks or portable media) is securely deleted; this can be arranged by contacting the IT Help Desk. Equipment must be assessed by IT services before being given to a new user or being disposed of.

All IT equipment must be disposed of securely, with the necessary contracts, processes and audit trails in place to ensure the confidentiality of any data stored on the equipment being disposed of.

Internet and Email Security

When accessing the Internet or email the following must be adhered to;

- Before using the Internet, Intranet or email for the first time all staff must accept the terms and conditions of the N3 Information Governance Statement of Compliance and HSCN Connection Agreement
- No illicit or illegal material may be viewed/downloaded or obtained via the

Internet or email

- Any material downloaded must be virus checked automatically by the system's anti-virus system
- The user will make their system available at any time for audit either by the IT department or internal and external audit
- Use of internet hosted services e.g. survey monkey for confidential information and/or PCD require approval of SIRO/ IG Group and may require risk assessments and a Data Protection Impact Assessment (DPIA)

Usage is monitored by the CCG and any breaches of security, abuse of service or non-compliance with the N3 Information Governance Statement of Compliance and HSCN Connection Agreement or organisational policy may result in disciplinary action, as well as the temporary or permanent withdrawal of all N3 services including email. More detailed guidance can be found in the Email and Internet Policies.

Assurances from IT Service Suppliers

The CCG will obtain regular assurance from Core IT providers that CareCert Alerts are being acted upon and are being addressed appropriately.

10.6 Sharing confidential information without consent

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

- Discuss the request with the appropriate CCG personnel such as the Caldicott Guardian and/or SIRO.
- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the individual to whom the information relates.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- Follow any locally agreed Information Sharing Protocols and national guidance.
- Seek advice from DPO' in case of doubt and where situation not covered by existing protocols.

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

- The police or another enforcement agency where the appropriate DPA Schedule 2 (formerly section 29) request form (in line with the Access to Records Procedure) or court order needs to be submitted from the law enforcement agency in order for the CCG to consider the request.

The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

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

10.6.1 National Data Opt Out

The national data opt-out was introduced in May 2018, following recommendations from the National Data Guardian. People can opt out of having their confidential patient information shared for reasons beyond their individual care, for example for research and planning on the coronavirus (COVID-19) outbreak. National data opt-outs are held on the NHS Spine against an individual's NHS number. If your use or disclosure of data needs to have national data opt-outs applied, you must remove records for patients with an opt-out registered from the data being used. The deadline for health and care organisations to comply with national data opt-out policy is now 30 September 2021. The deadline has been extended again, to enable health and care organisations to focus their resources on the coronavirus (COVID-19) outbreak.

10.7 Confidentiality and conversations

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

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

10.8 Records management

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

10.9 Access to records

Individuals have a right to request access to their records in line with the Data Protection Act and the General Data Protection Regulation by making a Subject Access Request. All staff should familiarise themselves with the CCG's Access to Records Procedure which should be followed for all requests for personal data. This procedure also gives guidance in relation to requests for the records of deceased persons under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

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

10.10 Information sharing

The organisation will ensure that information sharing takes place within a structured and documented process e.g. Data Protection Impact Assessment (DPIA) and in line

the General Data Protection Regulation (GDPR), the Data Protection Act 2018,the Information Commissioner's Code of Conduct and in accordance with the Health and Social Care Act 2018.

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

10.11 Information confidentiality incidents

A data protection breach is a breach of security which has led to the personal data of an individual, or group of people, being unlawfully or accidentally destroyed, lost, altered, disclosed or accessed by an unauthorised party.

All reportable Data Security and Protection breaches, including cyber security breaches (including but not limited to, physical destruction or damage to the organisations computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported to the Information Commissioner's Office (ICO) without delay and no longer than 72 hours after the incident came to light.

Incidents will be managed in accordance with the CCG's Incident Management and Reporting Policy.

Breaches should be:

- Notified immediately to the CCG's Information Governance team
- Detailed on the CCG's IR1 form
- If deemed reportable by the Corporate Governance Team, reported to the NHS Digital, Information Commissioner's Office via the DSPT incident reporting tool (external reporting will be co-ordinated by the CCG's Corporate Governance team and approved by the SIRO).
- Investigated and reviewed in accordance with the guidance in the checklist
- Reported publicly through the CCG's Annual Report and Governance Statement

For more information on what should be reported please see NHS Digitals incident reporting guidance at: https://www.dsptoolkit.nhs.uk/Help/29

10.12 Data Protection Impact Assessment

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

- Identify privacy risks to individuals
- Protect the CCG's reputation
- Ensure person identifiable data is being processed safely.
- Foresee problems and negotiate solutions.
- The CCG's procedure for DPIA should be followed.

11 Dissemination, implementation and training

The Data Security and Protection Toolkit (DTSP) requires that all staff must undergo information governance training annually. All staff will receive information governance in accordance with the IG Training Needs Assessment (TNA).

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

Additional training may be provided for those with special responsibility for data protection. The need for additional training should be identified with reference to the IG Training Needs Analysis.

Following ratification by the Audit and Governance Committee this policy will be disseminated to staff and made available on the CCG's intranet and website.

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

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

12 Review and monitoring

An assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT), which includes the requirements of GDPR, will be undertaken each year.

Reporting on information governance developments, risk, issues and incident is provided to all standard meetings of the Audit & Governance Committee (three per annum).

13 Public sector equality duty

The Equality Act 2010, available on the GOV.UK website, includes a general legal duty to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act
- advance equality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not share it

The protected characteristics are:

- age
- disability
- gender reassignment
- marriage or civil partnership (only in respect of eliminating discrimination)
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

All policies should include a statement that the CCG aims to design and implement services, policies and measures that meet the diverse needs of our service users, population and workforce, ensuring that no one is placed at a disadvantage over others.

In this statement also describe any elements of the policy which aim to reduce any inequalities experienced by any group(s) of people with any of the Equality Act Protected Characteristic(s).

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

THIS.InformationGovernance@this.nhs.uk

14 Consultation

Describe how consultation has or will take place with internal and external stakeholders.

If extensive consultation is not required, it may be sufficient to record this information in the version control table ('circulation' information).

15 References

This policy should be read in conjunction with:

Information Governance Framework
Privacy Notice published on the CCG's website
Records Management Policy (in draft)
Freedom of Information Act and Environmental Information Regulations Policy
Disciplinary Policy and Procedure
Anti-Fraud, Bribery and Corruption Policy Raising Concerns Policy
Internet and Social Media Policy
Access to Records Procedure
Freedom of Information Procedures
Data Protection Impact Assessment (DPIA) Checklist and Guidance
Safe Transfer Guidelines and Procedure
Incident Management, Investigation and Reporting Procedures

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

16 Appendices

Appendix A- Data Protection Principles

Appendix B- National Data Security Standards

Appendix C- Caldicott Principles

Appendix D- Password Guidelines

Appendix E- New Starter / Data Security & Protection Declaration Form

Appendix A

Data Protection Principles:

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

It is important to note that the regulations specify that:

- data processors can be held liable for breaches
- all actual information breaches must be reported via the IG Toolkit (to the ICO) within 72 hours of becoming known
- the penalty for breach of the regulations is now capped at a maximum of €20,000 (£17,000,000) or 4% of the turnover of an organisation
- organisations must employ the 'privacy by design' approach to activities involving personal data. A Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- fair processing notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU
- the consent model for processing personal data is to be further defined (see Caldicott 3 report and corresponding consultation and direction from the Department of Health)
- as part of the implementation of the regulations, a register of data controllers, will no longer be maintained by the ICO and organisations will not be required to complete/renew an annual submission
- data subjects have the new right to erasure, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within 30 days and provided free of charge (unless a request is "manifestly unfounded or excessive")

Appendix B

National Data Guardian Standards

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Appendix C

Caldicott principles:

Principle 1: Justify the purpose(s) for using confidential information Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law. Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

.

Appendix D

Password Guidelines

Standard user account passwords should contain a minimum of 10 characters.

No complexity of characters enforced, i.e. capital letters, digits, special characters such as '@'.

Passwords should not consist of well-known or publicly posted identification information. Names, and ID numbers are examples of well know identification information that should not be used as a password. The recommendation is 3 or 4 memorable words or a passphrase that excludes personal data e.g. 'Table Snow Golf' or 'I Want a new mountain bike"'.

Users should be prohibited from re-using previously used passwords and passwords should never be shared with anyone else.

The password only needs to be changed if the user requires this or if there is a suspicion of a breach.

Where 5 unsuccessful password attempts are made, the account should be locked and must then be reset by THIS Servicedesk.

Passwords should be memorised and never written down or recorded along with any corresponding account information or usernames.

Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to that application.

Care should be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. The username and password(s) used for your CCG/GP systems accounts should never be used for any personal accounts and services e.g. Amazon, Facebook etc.

When a password is provided to an authorised user, for the first time the user must be required to change that password when they first logon onto the system.

Appendix E

New Starter Information Governance Declaration Form

I confirm that I have received the **Information Governance / Data Security & Protection User Handbook** and understand that it is my responsibility to read and understand it and to raise any queries or concerns with my line manager or directly with The Health Informatics Service (THIS) Information Governance Team at: THIS.InformationGovernance@this.nhs.uk

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

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

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

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

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

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