NHS
Bolton
Clinical Commissioning Group

Bolton CCG
Data Security / Information Governance Staff Handbook

Policy Number	**IG008**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**July 2019**
Last Review Date	**June 2019**
Next Review Date	**June 2021**
Policy Author	**IG Team**
Version Number	**4.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	Sept 13	G Birch M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
1.1	August 2015	IG Team	Reviewed – Adopted from NHSE IG Staff User Handbook. Content and style changed.
2.0	October 2015	IM & T Ops	Approved
2.1	September 2016	IG Team	Reviewed – Minor admin changes. Contact details updated. CSU changed to GMSS
3.0	September	IM & T Ops	Approved
3.1	June 2019	IG Team	Complete Review – incorporating National Data Guardian Data Security standards, GDPR and DPA 2018
4.0	June 2019	IG Board	Approved
4.1	July 2019	CCG Chief Officer	Approved

Contents

1. INTRODUCTION

NHS Bolton Clinical Commissioning Group (will be referred throughout this Handbook as the CCG) has a statutory duty to safeguard the personal confidential data it processes. The principle of this handbook is to provide guidance and refer to the relevant data security policies and procedures in order for CCG staff to comply with data security legislation and national standards such as the National Data Guardian Data Security standards, the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018).

Although the Health and Social Care Act 2012 limits the amount of personal data a CCG can process, CCG's do still process a considerable amount of personal data, for example, staff data, teams who provide a direct care service such as Continuing Health Care, Medicines Optimisation and Safeguarding as well as when the CCG processes data when asked to do so to deal with complaints, processing personal information requests, national mandates set by NHS England and / or serious incidents. The CCG also process pseudonymised data which must also remain confidential especially where this can be re-identified within the CCG. GDPR class this as personal data in such cases. Information about the organisation itself can also be deemed sensitive in nature and not disclosed to unauthorised third parties.

Therefore, all information must be treated securely to ensure it is kept confidential when it needs to be, available when required and to those who have an authorised need to access and has integrity so the information can be relied upon and used efficiently and effectively. This is also known as the CIA (Confidentiality, Integrity and Availability) triad.

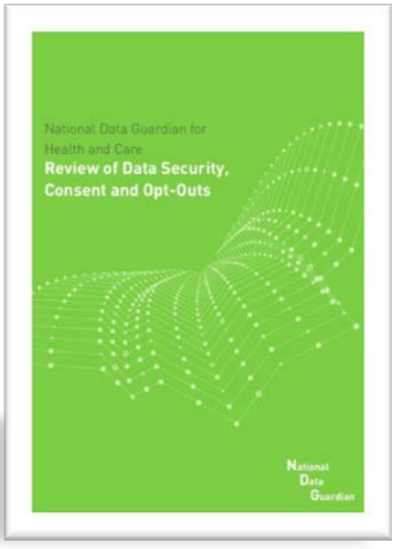
This handbook applies to all staff working for or on behalf of the CCG. Therefore such staff, whether as a Data Controller or as a Data Processor for others, shall be undertaken in accordance with laws and national standards for the NHS to protect personal information processed during the course of their work. These include (but are not limited to):

- Common law duty of confidentiality
- General Data Protection Regulation 2016

- Data Protection Act 2018
- Digital Economy Act 2017 regarding the annual data protection registration and fee
- Professional codes of conduct
- Privacy and Electronic Communications Regulations 2003 – soon to become thee-privacy regulations
- Caldicott
- National Data Guardian Data Security Standards
- Access to Health Record Act 1990
- Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- Confidentiality: Good Practice in Handling Patient Information (GMC 2017)
- Government Response "Your Data, Better Security, Better Choices, Better Care" July 2017
- Health & Social Care Act 2012
- Health & Social Care (Safety & Quality) Act 2015
- Human Rights Act 1998
- Records Management Code of Practice for Health & Social Care (2016)
- Manual For Caldicott Guardians (2017)
- Privacy & Electronic Communications Regulations (e-privacy – came into force in 9th January 2019
- Report on the Review of Patient-Identifiable Information (1997) *(The Caldicott Report)*
- Information: To Share or Not to Share (2013) *(Caldicott 2)*
- Review of Data Security, Consent and Opt-Outs (2016) *(Caldicott 3)*
- Safe Data, Safe Care – Care Quality Commission (2016)

This handbook provides guidance to ensure that all personal and special category of data is processed fairly, lawfully and as transparently as possible so that patients and staff are provided with assurance and can:

- Understand the reasons for processing personal and special category of data
- Gain trust in the way the CCG handles information
- Understand their rights to access information held about them.



The CCG also demonstrate the above by the publishing of a Privacy Notice which you can find on the website (http://www.boltonccg.nhs.uk/how-we-do-things/how-we-use-your-information).

Complying with the above standards ensures the information is processed legally, securely, efficiently and effectively, in order to deliver the best possible care.

The National Data Guardian Data Security standards will form the baseline for this handbook as these also cover compliance with GDPR and DPA 2018. These were created from the third review undertaken by Dame Fiona Caldicott, the previous national Caldicott Guardian, who is now known as the National Data Guardian (NDG) for Health and Care, in

2016. This review made recommendations to the Secretary of State for Health aimed at strengthening the safeguards for keeping health and care information secure and ensuring the public can make informed choices about how their data is used. The NDG outlines new data security standards for the NHS and social care, a method for testing compliance against the standards, and a new opt-out to make clear how people's health and care information will be used and in what circumstances they can opt out.

The full report is called Review of Data Security and Opt Outs, and can be accessed on the link below.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

The national guidance for the NHS coincides with the implementation of GDPR and DPA 2018 and encompasses the spirit of this legislation.

In this handbook, there will be a dedicated section for each Data Security Standard to assist with compliance with hints, tips and links to policies, procedures, templates and websites where detailed and / or additional information can be found.

2. DATA SECURITY STANDARD 1 – PERSONAL CONFIDENTIAL DATA

This standard states that,

This section provides guidance and links to further information on:

- Leadership, Accountability and Key Data Security roles
- Legislation, policies and procedures
- Records of data processing – Information Asset Register and Data Flow Mapping Registers
- Individual Rights
- Data Protection by Design / Data Protection Impact Assessments (DPIA's)
- Data Quality
- Records Management
- Information Sharing
- Anonymisation and Pseudonymisation
- National Data Opt-out

2.1 Leadership, Accountability and Key Data Security Staff

In order for the implementation of GDPR to be successful, it requires CCG leaders to buy into and support the changes necessary to maintain and improve practices. The highest level of management need to be routinely briefed regarding data security compliance and accountability and oversight needs to be stated at a senior level to ensure there is buy in. These key roles are listed below:

Chief Officer

The individual with overall accountability for Data Security within the CCG is the Chief Officer. The role is to provide assurance, via reporting mechanisms to the Governing Body that data security and compliance with GDPR / DPA 2018 is being maintained and improved where necessary. The key reporting tool is the Data Security and Protection Toolkit. The CCG's Chief Officer is Su Long.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) must be an Executive Director or other senior member of the board. The CCGs SIRO is also the Chief Finance Officer. The SIRO acts as an advocate for information risk, owns the information risk policy and understands how the strategic goals of the CCG may be impacted by data security risks. They also ensure that information assets have an assigned information asset owner (IAO). The SIRO is supported by the organisation's Information Asset Owner's and IG Team (see below). The CCG's SIRO is Ian Boyle.

Caldicott Guardian / National Data Guardian

The Caldicott Guardian has an advisory role for protecting confidentiality and ensuring personal data is shared appropriately and securely. They are required to be registered on the National Register of Caldicott Guardians. The Caldicott function is supported by the organisation's IG Team.

Please note the national Caldicott Guardian title has changed to the National Data Guardian and this is still appointed to Dame Fiona Caldicott. The CCG's Caldicott Guardian is Dr Jane Bradford.

Data Protection Officer (DPO)

The GDPR requires all public authorities to nominate a Data Protection Officer (DPO). This role requires them to have reporting channels directly to the highest level of management and they must have the requisite professional qualities and expert knowledge of data protection compliance. They assist with the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for citizens and the Information Commissioner's Office (ICO). The DPO is supported by the organisation's IG Team. The CCG's DPO is Mike Robinson.

Information Governance (IG) Team

The IG Team is responsible for ensuring that the Data Security programme is implemented and maintained throughout the CCG, including the completion and annual submission of the organisation's Data Security & Protection Toolkit (DSPT). They also supports the organisation in coordinating and managing Data Security (IG) breaches / incidents, offering bespoke data security (GDPR) advice and guidance, ensure there is awareness of data security, ensure appropriate data security training is delivered to staff according to their duties, liaise with networking and other committees to ensure compliance with the law and national standards, ensure the organisation complies with data security legislation, policies and procedures and provide expertise for the resolution / discussion of IG issues.

Information Asset Owners (IAO's)

The SIRO is supported by Information Asset Owners. Their role is to understand what information is held, how it is managed and who has access, and why, to information systems in their own area. As a result they are able to understand and address risks to the information assets they own and to provide assurance to the SIRO on the security and use of those assets. GDPR requires that records of information processing are undertaken therefore it is essential that IAO's review / maintain and update their Information Asset Registers and Data Flow Mapping Registers as and when required. The IG Team support the IAOs in fulfilling their role.

Information Asset Managers (IAM's) and Administrators (IAA's)

An IAO may delegate responsibility for management of confidential information to an Information Asset Manager (IAM) or Information Asset Administrator (IAA). While the IAM and IAA may be responsible for the proper handling of information, the IAO remains

accountable**,** therefore the IG Team will need to ensure that the IAM and IAA understands, and has the required competencies to undertake these responsibilities.

Delegated responsibilities typically include:

- Managing the joiners, movers and leavers process within the team
- Ensuring all team members keep their training up-to-date
- Granting and revoking access to confidential information
- Recognising potential or actual security incidents
- Consulting the IAO on incident management
- Ensuring that risk assessments and other documents for the study are accurate and maintained

IT Technical / Security Staff

IT technical staff ensure that the technology we use is safe and secure. They provide advice, guidance and support regarding any IT technical issues. The IT provider currently ensures that cyber security standards are in place to prevent / detect and deter cyber-attacks as much as possible

The above lists the key staff in order to ensure data security is maintained and improved but all staff have a role to play and a duty to ensure information is processed securely and confidentially.

2.2 Legislation, Regulations, Guidance and Organisation Policies

Staff must be aware of the key legislation and national standards regarding Data Security.

The key laws and standards are listed below:

General Data Protection Regulation 2016

This was applicable in UK law from 25th May 2018 coinciding with the UK Data Protection Act 2018. The GDPR applies to Data Controllers and Data Processors who process personal and / or special category of data. It applies to automated and manual filing systems where personal data are accessible (e.g. chronologically ordered sets of manual records). Pseudonymised data e.g. key-coded data could also fall into the scope of GDPR depending on how difficult it is to associate the pseudonym to a particular individual.

GDPR states that you must have a lawful basis for processing personal data (Article 6) and a condition for processing special category of data (Article 9). There are also stronger conditions for using consent to process personal data, strengthened individual rights, the need to appoint a DPO, the need to document record processing activities (Information Asset Register / Data Flow Mapping Register maintenance), requirement to ensuring openness and transparency (ensure privacy notices are in place), the need to ensure data protection by design principles are in place, ensure adequate organisational and technical security is in place, ensure incidents are reported and also to comply with the seven principles which are:

Article 5 – GDPR Principles

Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

The organisation must show transparency regarding how information is processed and the most common format of demonstrating this is via the production and dissemination of a privacy notice. The organisation has a privacy notice available via the website which documents information processing activities.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a matter 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;

Only use personal information obtained by the organisation in connection with the business of the organisation and ensure information is not used for any purposes other than originally intended.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes of which they are processed;

Only obtain the minimum amount of information and do not obtain information which is not needed.

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Ensure that all information entered either manually or electronically is accurate, and where recorded elsewhere ensure that there are appropriate procedures in place to continually review and update the different sources, to ensure accuracy and version control. Where possible do not hold duplicate copies as this increases the risk of inaccurate information being held.

(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 interests, 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;

All records are affected by this article regardless of the media within which they are held and / or stored. For further guidance please see the organisation's Records Management Policy. When disposing of personal information use only the confidential waste destruction process.

(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;

Examples or which are:

- Do not allow unauthorised access.
- Do not share passwords.
- Do not leave confidential information on your desk or post trays and ensure all paperwork is tidied away when not in use or at the end of the day.
- Ensure that computer / laptop screens are locked when away from the desk

The seventh principle Article 5 (2) state that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the [above] principles."

Once again, transparency and accountability are key under GDPR. We must tell people what we do with personal data and be accountable for how we process this and thus is must be undertaken securely and confidentially at all times.

Data Protection Act 2018

The Data Protection Act (DPA) 2018 sits along with the General Data Protection Regulation (GDPR) governs how we collect, store, process and share data in the UK.

The DPA 2018 was enacted on 23rd May 2018 (2 days prior to GDPR). The DPA 2018 fills in the gaps where flexibility and derogations are permitted in the UK. It will ensure that the provisions in the GDPR will be applicable in the UK post Brexit. It is important to note that the DPA 2018 does not replicate all the provisions in the GDPR but cross-refers therefore it is necessary to view both side by side in order to see the complete picture of all data protection legislation.

Under GDPR, the CCG no longer has to register with the ICO but under the Charges to Information Regulations 2018 (Digital Economy Act 2017) it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work.

The Data Protection Act 2018 also covers areas of information processing relating to:

Law enforcement processing

- Provides a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes.
- Allows the unhindered flow of data internationally whilst providing safeguards to protect personal data.

Intelligence services processing

- Ensures that the laws governing the processing of personal data by the intelligence

services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and enforcement

- Enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allows the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.
- Empowers the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

Caldicott Principles

In 2013, when the second review was undertaken within the NHS regarding data processing following issues with information sharing and data losses, the following principles were adopted which are

Principle 1 – Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 – Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 – Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 – Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Comply with the Law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality

Health and Social Care professionals should have the confidence to share information in the best interests of the patients within the framework set out by these principles.

Since this review, a third review was undertaken by Dame Fiona Caldicott as outlined in the Introduction which introduced the 10 National Data Guardian Data Security Standards which are:

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

- **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.

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

- **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.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.

- **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.

These standards form the basis of the new Data Security and Protection Toolkit which gives assurance regarding compliance with them and also GDPR.

Data Security & Protection Toolkit (DSPT)

NHS Digital manages, on behalf of the Department of Health, the Data Security and Protection Toolkit (DSPT). This replaces the Information Governance Toolkit (IG Toolkit). It allows the CCG to demonstrate that they can be trusted with the confidentiality and security of personal data. The DSPT is:

- a self-assessment online tool mandated for use by NHS, Social Care, GPs, commercial third parties and other providers of NHS / Healthcare-related services to self-audit their Data Security (IG) compliance
- is based on the 10 National Data Guardian Data Security standards. From this, the DSPT is made up of a number of assertions and evidence items depending upon the size and type of organisation
- a baseline to maintain and develop an annual Data Security (IG) compliance work programme each financial year, facilitated by the IG Team.
- subject to both internal and external audit (deep dives).
- has reports available showing compliance with the National Data Guardian (NDG) standards

For more information, please visit:

https://www.dsptoolkit.nhs.uk/

Policies and Procedures

In order to provide staff with guidance on the legislation and national standards, the IG Team have produced the following policies and procedures. You will be able to find these on the CCG Website:

- Information Governance Policy
- Confidentiality and Data Protection Policy
- Data Protection by Design Compliance Checklist
- Data Protection Impact Assessment Template and Guidance
- Data Quality Procedure
- Data Security & Protection Breaches / Incident Reporting Policy and Procedure
- Information Governance Framework (IG Framework)
- Data Security / Information Governance Training Needs Analysis
- Confidentiality Audit Procedure
- Individual Rights Procedure
- Information Sharing Agreement Template
- Privacy Notice for Patients & the Public
- Privacy Notice for Staff
- Records Management Policy
- Secure Transfers of Data Procedure
- Information Risk Policy
- Information Governance Clause

2.3 Records of Data Processing – Information Asset Register / Data Flow Mapping Register

An important aspect of GDPR is ensuring that there is a record of data processing activities (Article 30). This is achieved by ensuring the Information Asser Register and Data Flow Mapping Register is populated with this information and regularly reviewed / updated where necessary. These are saved locally by the IG team.

In addition, we now need to be transparent about what the legal basis is for processing personal data under Article 6 and what the condition is for processing special categories of data (previously known as sensitive data such as health data and employment data) is under Article 9. To remind you what these are, they are listed below.

Article 6 – the legal basis for processing personal data under GDPR / DPA 2018

(1)(a) - Consent
(1)(b) - Contractual Necessity
(1)(c) - Compliance with legal obligations
(1)(d) - Vital Interests
(1)(e) – Performance of a task carried out in public interest or in exercise of official authority – this is the main one we use within the CCG to carry out our statutory duties for processing personal data, for example, to process personal data when this relates to healthcare such as Continuing Healthcare and to process personal data relating to employment by our Human Resources department
(1)(f) - Legitimate Interests

Article 9 – the conditions for processing special category of data

(2)(a) - Explicit Consent
(2)(b) – Employment – this is the condition we use within the CCG to process employment data
(2)(c) - Vital Interests
(2)(d) - Charity or not for profit bodies
(2)(e) - Manifestly made public by data subject
(2)(f) - Legal Claims
(2)(g) - Substantial public interest
(2)(h) - Health and Social Care – this is the condition we use within the CCG to process healthcare data when this relates to direct care such as Continuing Healthcare
(2)(i) - Public Health
(2)(j) – Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes – see Article 89 (1)

The IG team will ensure that you regularly check the information on both registers is correct and up to date especially when you have new systems / processes / assets / transfers or access to personal data.

2.4 Individual Rights

GDPR has introduced strengthened rights for individuals under GDPR. In summary, these are:

Right to subject access - individuals can request access to information the CCG process about them. The timeframe for responding with the information is 1 calendar month and no fee can be charged (unless exemptions apply). Under GDPR, organisations must now provide additional information about the processing of personal data when responding to a subject access request. In summary, this is an explanation of the categories of data being processed, the purpose of such processing, and the categories of third parties to whom the data may be disclosed. This is documented in the privacy notice so you can provide a copy of this on responding.

Right to rectification - ask for inaccurate information to be corrected and must comply within one calendar month.

Right to objection - individuals have the right to object to processing data about patients and staff. However, please note if the CCG can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If the CCG didn't process any information about you and your health care (where the organisation process health data) it would be very difficult to provide care and treatment. Where this applies for direct marketing, this is an absolute right and in such cases the organisation must comply immediately and where automated processing used.

Right to restriction on processing - individuals have the right to restrict processing where accuracy is contested, data controller no longer needs data but subject requires it to be kept for legal claims and individual has objected pending verification of legitimate

grounds and other national programmes such as NHS Digital national opt-out.

Right to Data Portability - Only if the CCG have your explicit consent for any processing we do, you have the right to have data provided to you in a format you have requested such as in an excel spreadsheet, csv file format.

Right not to be subject to a decision based solely on automated processing - The CCG (at this time) do not process data using this method, so this right will not apply to our data processing activities.

Right to withdraw consent - individuals have the right to refuse (or withdraw) consent to information sharing at any time when the CCG asks for consent. However, this may not be possible if the sharing is a mandatory or legal requirement imposed on the organisation. Any restrictions, and the possible consequences of withholding your consent, will be fully explained to you as the situation arises.

Right to complain - If you feel that your personal data the CCG processes at the organisation has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of personal data, please contact the Data Protection Officer and / or IG Team in the first instance to rectify this. If you are still unhappy with this response and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

For more information regarding individual rights, please see the Individual Rights Procedure.

2.5 Data Protection by Design / Data Protection Impact Assessments

GDPR now requires that the CCG put in place relevant technical and organisational measures / processes to ensure the data protection principles are adhered to and also to safeguard individual rights. This is known as "data protection by design and by default." This principle applies organisationally and requires the CCG to take account of data protection considerations even before it is decided whether the processing is likely to result in a high risk or not to individuals (which is principally what a Data Protection Impact Assessment (DPIA) is aimed to address). Data Protection by Design is not just the completion of a Data Protection Impact Assessment it involves all the measures that can be taken to ensure that data is protected, secure and confidential from when the idea of using personal data is originally thought about.

<u>Data Protection Impact Assessment (DPIA)</u>

GDPR places a new obligation to do undertake a Data Protection Impact Assessment (DPIA) when the processing is likely to result in a high risk to individual's rights and freedoms relating to their data. The aim of a DPIA is to assist in identifying data protection issues and risks before implementation so this can be rectified or in some extreme cases stopped. The CCG completes these for all new or changes to systems / processes / assets where personal and / or special category data is to be processed. In cases where high risks are identified, the Information Commissioners Office (ICO) must be consulted.

For further information about Data Protection by Design and the Data Protection Impact Assessment, please see the:

- Data Protection by Design Compliance Checklist
- Data Protection Impact Assessment Proforma and Guidance

2.6 Data Quality

The CCG recognises that decision making at every level within the NHS whether this is financial, clinical or managerial needs to be based on information which is of the highest quality and integrity. The information used in the CCG is derived from a multiple range of sources either on paper or electronically and the CCG must ensure that they have the assurance that information they produce or use from another source is of the highest quality.

Data quality is crucial and the availability and integrity of complete, accurate, relevant, accessible and timely data is important in supporting the aims of the CCG such as supporting patient care, managing staff, performance monitoring and management and planning of healthcare services. It also portrays accountability.

Careful monitoring and error correction can support good quality data, but it is more effective and efficient for data to be processed correctly the first time. In order to achieve this, procedures such as this must exist so that staff are aware of the importance of data quality.

Where staff process data they need to ensure that this is of the highest quality it can be by ensuring it is accurate, up to date and that validity checks are made to ensure it remains as such. This is especially important when personal data, special categories of data and business sensitive data is processed.

For further information, please see the Data Quality Procedure.

2.7 Records Management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal. The organisation has a statutory obligation to maintain accurate records of its activities which are public records under the Public Records Acts 1958 & 1967.

The Records Management Code of Practice for Health and Social Care (published by the Information Governance Alliance in July 2016) is a guide for use in relation to the practice of managing 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. It also outlines retention periods for health and corporate records to be adopted by the CCG.

https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

GDPR requires improved records management. Organisations need to know what personal data they hold (this must be logged on an Information Asset Register), be able to access it when they need to, know how long they need to keep it for, ensure they keep it secure when needed and dispose of securely or archived securely when no longer

required or when the retention period is met. Organisations must also show transparency and tell individuals what data they hold and who they share it with (by use of privacy notice).

The NHS has at least two categories of records, clinical / health and corporate:

- **Health / clinical records -** A health record is defined as being any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

- **Corporate records -** are defined as anything that contains information in any media, which has been created or gathered as evidence of undertaking of work activities in the conduct of business. Corporate records may also be generated through supporting patient care and can also be generated through agency/casual staff, consultants and external contractors.

For further information regarding records management please see the Records Management Policy.

2.8 Information Sharing

Who can you share information with, and what information can you share? Sometimes staff often get confused as regards what they can and cannot share. Remember that GDPR and IG are not barriers to appropriate sharing. This has since improves since the new Caldicott principle was introduced in 2013 which stated that,
'**The duty to share information can be as important as the duty to protect patient confidentiality'.**

This is the guiding principle when considering the sharing of patient information.

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The organisation must ensure that mechanisms are in place to enable reliable and secure exchange of data within legal limits.

Seven golden rules of Information Sharing are:

1. Remember that the GDPR, DPA 2018 and Human Rights Act 1998 are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, the IG Team / DPO, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and DPA 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You

will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Sharing for direct care purposes

Staff sharing personal information with other organisations for direct care purposes do not necessarily need an Information Sharing Agreement in place but it is good practice to have one and to also log this information on the Data Flow Mapping Register.

Sharing for non-direct care purposes

Information Sharing Agreements are required to be put in place when information is being shared for a non-direct care purpose and this must specifically state the legal basis or overriding interest for sharing.

For further advice and guidance regarding information sharing and to obtain a copy of the Information Sharing Agreement template, please contact the IG Team.

2.9 Anonymisation / Pseudonymisation

Information that is to be used or shared for non-care purposes must be anonymised unless you have a legal statute which applies use of personal data and documented and in such cases must be documented in an Information Sharing Agreement. Anonymisation is defined by the ICO as the process of turning the data into a form which does not identify individuals and where identification is not likely to take place. This may include research, commissioning and assessing the quality and efficiency of services. If the purposes can be achieved with anonymised information then they must be. This means that the information will have all identifiable information that may identify an individual permanently removed from it.

Pseudonymisation within a trusted and safe environment may be an acceptable alternative. This is similar to anonymisation, and is defined by the ICO as the process of giving individuals in a dataset a unique identifier which does not reveal their real identity. Whereas this is still defined as personal data under the DPA 2018, its use can help reduce privacy risks by making it more difficult to identify individuals.

If the need to use the information cannot be achieved by either anonymisation or pseudonymisation, then patient consent is generally required. The only exemption to this is if there is an overriding and statutory basis for breaching confidentiality. These include,

but are not limited to:

- Compliance with a Court Order
- Notifiable Diseases to Public Health England
- To support the prevention or detection of serious crime
- Under s251 of the National Health Service Act 2006 when ordered by the Secretary of State for Health and Social Care
- NHS Digital has powers to request information which are binding on health bodies, although such powers may not be enforced where a patient has objected.

These are complex issues which will typically require expert advice and consideration. Staff faced with decisions on such matters should have regard to national guidance and seek advice from the DPO and / or IG Team.

2.10 National Data Opt-Out

The national data opt-out is a new service announced on 25 May 2018 by NHS Digital that allows patients to opt out of their confidential patient information being used for research and planning.

Patient information about the programme, including how to set their opt-out choice is available click here.

Staff can download leaflets, posters and other resources to use when informing patients here.

The national data opt-out was introduced to allow patients to opt-out from the use of their data for research or planning purposes. This is provided in line with the recommendations of the National Data Guardian, Dame Fiona Caldicott, in her Review of health and social care Data Security, Consent and Opt-Outs. The service is currently in a process of continual development.

By 2020, all health and care organisations will be required to apply national data opt-outs where confidential patient information is used for research and planning purposes. NHS Digital have been applying national data opt-outs since 25 May 2018.

The national data opt-out replaces what were previously known as ‘Type 2’ opt-out,

3. DATA SECURITY STANDARD 2 – STAFF RESPONSIBILITIES

This standard states that,

This section provides guidance and links to further information on:

- Induction Policy - IG
- Confidentiality in the NHS
- Data Security Hints and Tips for the workplace
- Staff Contracts / Confidentiality Code of Conduct
- Staff Awareness / Briefings / Communications

3.1 Induction Policy - IG

All new starters receive a face to face CCG induction from their line manager. Part of the induction covers the following areas:

- Informed about the requirement to complete Mandatory Data Security / IG training (Data Security Awareness) available at https://boltonft.traineasy.com
- Informed of the location of the Data Security Policies / Procedures / DPIA template / historic advisories / bulletins / ICO Codes of Practice
- Confidentiality Code of Conduct discussed and informed of correct procedure
- Data Security (Information Governance) general discussion and advised who to contact if any questions have
- Advised that the CCG monitor compliance and undertake regular audits for example to ensure screens are locked and paper work is put way etc.
- Advised of the location of the Data Security Breaches - Incident Reporting Procedure and informed who to contact should a data security (IG) Incident take place
- Advised to contact the IG Team at any time if have any questions.
- Advised where a copy of the Staff Privacy Notice can be found and informed of the location of the Patients & Public Privacy Notice

3.2 Confidentiality in the NHS

The Common Law Duty of Confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, for safeguarding reasons, or where there is a statutory or Court Order to do so. This provides the baseline regarding how we process data in the NHS. Sharing and use of information about individuals within and between partner agencies is vital to ensure co-ordinated and seamless provision of direct care to patients. Explicit consent is not required under GDPR; however, practitioners must maintain an awareness of the Common Law Duty of Confidentiality, that if the patient disclosed information in circumstances where it was expected that a duty of confidence applied, it

should not normally be further disclosed without the individual's consent. If this has not been obtained it is the responsibility of the member of staff intending to share personal information to make and document an appropriate decision based on whether disclosure is essential to safeguard either patient or a third party, is considered to be in the public interest, or if there is a legal obligation to share the information, such as a Court Order.

In addition to the above, confidentiality in the NHS has also been guided for the last 15 years by the Confidentiality NHS Code of Practice (2003). Despite its age, this is still a current document that sets out required standards of practice concerning confidentiality. To view, please click on the link below:

https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

In 2013, the Health and Social Care Information Centre (now known as NHS Digital) produced a document entitled '**A guide to confidentiality in health and social care – Treating confidential information with respect**'. This outlines 5 rules that the CCG must adhere to in relation to handling information. These are:

RULE 1: Confidential information about service users or patients should be treated confidentially and respectfully

RULE 2: Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

RULE 3: Information that is shared for the benefit of the community should be anonymised.

RULE 4: An individual's right to object to the sharing of confidential information about them should be respected.

RULE 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

To view, click on the link below:

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care

If the CCG collects, analyses, publishes or disseminates confidential health and care information, they must also follow the NHS Digital's Code of practice on confidential information. It clearly defines the steps that organisations must, should and may take to ensure that confidential information is handled appropriately. The code will help organisations put the right structures and procedures in place so that front-line staff follow the confidentiality rules. It provides good practice guidance to those responsible for setting and meeting organisational policy on the handling of confidential health and care information, such as board members.

3.3 Data Security Hints and Tips for the workplace

Following the principles below helps keep data secure and confidential:

Organisational Arrangements

Make sure you know the name of the following:

- SIRO
- Caldicott Guardian
- Data Protection Officer
- Information Governance Manager
- IT Lead

If you are unsure, please contact your IG Manager.

Office Environment

- Do not discuss confidential matters outside of work, during breaks in public areas, or with anyone at work who does not need to know it; be aware that other people may overhear, particularly in corridors and open plan offices / kitchens
- Do not leave working papers lying around the office – ensure these are securely locked away when away from a desk
- Remove documents from photocopiers immediately when printed especially if these are not printed via secure printers
- Hold keys and other access means, such as ID cards and combinations of locks, securely away from the point of use. Ensure that there is an appropriately secure system in place to allow access in event of emergency or and individuals absence
- Keep offices locked when unoccupied, and maintain overall building security. Be aware of people, whether staff, patients or general public, who may not have access to certain areas but try and 'tailgate' you into a secure environment
- Keep workstations and other computer equipment secure, being particularly careful with laptops when not in use, especially not leaving them unattended in vehicles or public places
- Lock away portable equipment when not in use
- Ensure cabinets containing personal data are locked when unattended
- Passwords must be a combination of letters and digits, and a combination of characters, typically using the lower case of the keyboard. Some systems require you to use special characters, such as '?' and '!';
- Passwords must not be written down
- Ensure that computer monitors cannot be seen by people, especially in public Reception areas
- Lock your computer when you are not using it, even for short periods, by using '**Ctrl-Alt-Del**', and selecting Lock from the options;
- Do not allow **anyone** else, including your line manager or IT, to use your log-on to any organisation computer or computer system. To do so breaches the Computer Misuse Act 1990.
- Access to all PCD whether held on paper or electronically must be restricted;
- Staff must ensure that security doors are closed properly and blinds drawn, and that

any door entry codes are changed regularly, ideally when a member of staff leaves the team or it is suspected that someone else knows the code;
- All staff must wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access. Visitors should be met at reception points and accompanied to appropriate member of staff or meeting and also should be asked to sign in and out of the department;
- On termination of employment or contract staff must surrender door keys / fobs and all relevant organisation equipment as part of the staff leavers' process;
- All computer assets including hardware and software must be recorded on an IT Asset Register that details the specification, user and location of the asset.

Availability and Access to personal data

- Access to records is based on the appropriateness of access by role, in line with GDPR / Caldicott Principle 4 and the National Data Guardian Data Security Standard 4 that access to personal data is on a strict need to know basis;
- There is no automatic right of access to records and access must be agreed in advance with the respective IAO.
- Do not store personal data on the hard drive of any laptop or PC. Always use network folders / drives that have access controls;
- Never send personal / confidential data outside the organisation without appropriate levels of authorisation or protection. Also, ensure this is logged on the Data Flow Mapping Register if this is a regular flow.

Accuracy, Retention and Disposal

- If adding or updating information to records, you must be able to satisfy yourself of its data quality such as the accuracy and relevance
- Records must be retained in line with **Records Management Code of Practice for Health and Social Care (2016)**;
- Ensure that records you process are also recorded on the Information Asset Register and state the legal basis for the use of these
- Ensure any unneeded PCD on paper is confidentially destroyed. Do not use it as scrap paper. Ordinary bins and 'recycling' bins must not be used for paper containing PCD – please use the confidential waste bins / consoles;
- Ensure that disposal of redundant equipment / IT kit is carried out securely by contacting the organisations IT Services Team to organise this

Transfers of data

For any transfers of data by various methods and media, please see the Secure Transfers of Data Procedure.

Requests for Information

If you receive a request for information about a patient, staff member, etc. and it is not usually part of your job to respond, you should:

- Refer requests for personal information immediately to your line manager or to the person who is designated to deal with such a request

- Refer any enquiries from the police to the IG Manager / Caldicott Guardian and / or DPO. The police and other law enforcement agencies do not have automatic right to access personal data about patients and staff, although the organisation does its best to co-operate with them when it is legal to do so. Article 11 of the Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the prevention or detection of crime and the apprehension of prosecution of offenders. Any request by the Police for access to information held about an individual must be accompanied by the relevant consent form from the Chief Superintendent of the requesting police force.

  The Crime and Disorder Act 1998 also allows (but does not require) the CCG to disclose information to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder. For the CCG to consider releasing any information without consent, the access request must relate to a serious crime in line with the Crime and Disorder Act 1998 (for example, murder or rape), otherwise the Police should be asked to obtain a Court Order or written approved signed consent.

  All such requests from the Police should be in writing and forwarded immediately to the Caldicott Guardian and the IG Manager.

- Requests from the media should be referred to the Communications Team;
- Guard against people seeking information by deception (social engineering), in particular, by checking the identity of people requesting confidential information and by following good practice guidelines for dealing with such requests.

Abuse of Privilege

- It is strictly forbidden for staff to look at, or seek, any information relating to themselves, their family, friends, acquaintances or colleagues unless they are directly involved in processing the information as part of their responsibilities as an employee;
- Information regarding patients or staff cannot be passed onto a third party unless for Direct Care purposes, with explicit consent or whether a legal exemption applies;
- Seeking out or looking at information or offering to sell information is an offence under Data Protection legislation and may attract disciplinary action that could result in dismissal. This applies to both patient and staff information;
- Organisation IT systems have an audit facility that monitors access to information held on that system, including ‘read only’ access. You may face disciplinary action if you are found to be accessing information that is not related to you role without good reason.

Disclosures

You may, as part of your job, legitimately need to disclose personal confidential data to others:

- Keep the amount of information disclosed, even within the NHS, to a minimum;
- Do not duplicate records, on paper or in a computer, unless absolutely essential;
- Advise those to whom you are legitimately disclosing PCD that they must not pass it

on;

- Ensure when PCD is disclosed to a non-NHS organisation that an agreed Information Sharing Agreement (ISA) is in place when necessary (see Chapter 21?). If in doubt contact the IG Team.
- Ensure that you check email addresses thoroughly if you are sending personal data.

Disposal / Deletion of Data / Confidential waste

All users must ensure that, where equipment is being disposed of, all data on the equipment / device is securely destroyed; this can be arranged by contacting the organisations IT Service Provider which is Bolton Hospital Foundation Trust.

Any paper documentation that is no longer required following transfer must either be filed away securely and / or securely disposed of using the confidential waste shredders situated in the CCG's office areas.

Social Media and the Use of Mobile Phone-based Messaging Apps

Transfers of business confidential information / personal data to social media platforms is not permitted. Only approved information by the CCG is published on social media platforms such as Twitter and Facebook. These platforms must not be used to transfer / store business information or discuss any work related **issues**.

On a general level, some simple advice, to keep yourself safe is to **NEVER:**

- Make friends with people of whom you are unsure;
- Reveal personal confidential data (PCD), including photos, about patients or colleagues;
- Moan about your employer, patients or colleagues;
- Discuss sensitive information;
- Upload compromising photos of yourself.

Plus, be extra careful if mixing work and private life on social media.

More specifically, messaging apps are useful and efficient if used correctly, and there is full encryption in place. Applications such as WhatsApp now have encrypted messages but some may not so please check with IT first. Benefits of using text applications are great if used appropriately when needing to communicate speedily, such as for the filling of rota gaps, or during major incidents. But,

- They must not be used as a work around for healthcare referrals / advice within or between organisations;
- The inclusion of PCD of any sort is unacceptable.

3.3 Staff Contracts / Confidentiality Code of Conduct

Staff have a duty to observe the Confidentiality Code of Conduct which outlines practices and behaviour ensuring adherence with data security legislation (GDPR / DPA 2018) and national standards such as the National Data Guardian Data Security standards. This supplements staff contracts of employment as these tend to focus on confidentiality and

not include the other areas of data security such as the integrity and availability of information.

It also provides links to key data security policies and principles for staff advice and guidance to comply with GDPR and provides confirmation to ensure that staff are aware of and agree to adhere to data security processes at the CCG. In addition, the code of conduct reminds you that usage of IT systems (particularly where personal data is processed) is logged and attributable to you.

If you are an administrator or authorise access to a system / data set, staff with this additional role need to complete the disclaimer for IT / System Administrators.

For more information, please contact the IG Manager.

3.4 Staff Awareness / Briefings / Communications

Staff are regularly informed about the data security work programme and made aware of key issues regarding GDPR / DPA 2018 compliance via a variety of methods. These include:

- News articles / briefings sent to staff via e-bulletin
- All IG documentation is available on the CCG website
- Verbal updates and key information disseminated to staff via the CCG Staff briefings / meetings

In addition and in accordance with the requirements of the DSPT, an annual staff survey is sent to all staff to complete. This survey informs the IG Team regarding current compliance with data security standards and where, if any, recommendations need to be made such as raising awareness about a specific new policy for example.

4. DATA SECURITY STANDARD 3 – TRAINING

This standard states that,

This section provides guidance and links to further information on:

- Data Security Training Need Analysis
- Data Security / IG Mandatory Training

4.1 Data Security Training Needs Analysis

The CCG has a Data Security Training Needs Analysis which identifies training requirements for all staff and especially for those who process personal data. This document is produced and signed off in conjunction with the DPO. Please ensure that you read the document and check that you have completed the necessary training for your role.

The SIRO / Caldicott Guardian and Data Protection Officer are required to keep their knowledge and skills up to date and attend a yearly data security training for their roles.

For further information, please see the Data Security / IG Training Needs Analysis.

4.2 Data Security Mandatory Training

All staff, who work for or on behalf of the CCG including new starters, existing staff, temporary workers, volunteers and contractors, must complete mandatory data security training. The CCG has a responsibility to ensure that all staff and in particular those working with patient and staff information are aware of the key data security legislation and national guidance and the risks to the reputation of the organisation which may occur, if processes are not followed.

For the CCG, the Data Security Awareness module is available via the Moodle E-Learning system on the Train Easy website, https://boltonft.traineasy.com. Passwords for the system can be reset on the e-learning portal by clicking on the Yes, help me log in button on the login page. If assistance is required staff are asked to e-mail e-learning@boltonft.nhs.uk.

This module has been updated to provide information on GDPR, DPA 2018 and core learning messages from the National Data Guardian's review. It offers the minimum requirements regarding data security awareness and no matter how good the training is, it can never capture all the unique local priorities and nuances. This training is therefore supplemented with briefings and communications as highlighted in section 3.4. In addition, if you are unsure always seek help from the IG Team / DPO.

5. DATA SECURITY STANDARD 4 – MANAGING DATA ACCESS

This standard states that,

This section provides guidance and links to further information on:

- Access to systems
- System Administrators
- Monitoring & Auditing

5.1 Access to systems

The CCG need to know which staff have access to systems that process personal confidential data and those which hold more than 100 records (as defined by the NDG Standard 4). In addition, the CCG need to know what access rights staff have, for example, some staff may have administrator rights and provide access / user accounts for other staff. Therefore, for each system using role-based access, the CCG need to know the following as outlined in the table below:

Sample System		
Role	**Description**	**Staff Names and Titles**
Admin	Ability to amend, delete and create new tables and look up fields	
General User	Ability to add amend and delete own related records and view others	
Super User	Ability to add, amend and delete own created record, amend and view others	
View User	Ability to view all records	
Backup User	Technical account used to archive the systems database	

It is also important to know if access to a system is managed by the system itself or use a form of federated access in which a single account is trusted across multiple IT systems such as Single Sign On (SSO).

This information must be supplied on the Information Asset Register and it is important that Information Asset Owners / Administrators input and check this information on the register and review it regularly.

5.2 System Administrators

System administrators by nature of their role have elevated rights compared to a normal user. Therefore, they have a great deal of system power and with great power becomes

great responsibility. The system administrator needs the highest level of integrity in terms of respect of the confidentiality, integrity and availability of the systems they support. Administrators are therefore accountable for that responsibility. In order to ensure that administrators are aware of this duty, they are reminded when given this responsibility they are accountable to the highest standards of use.

5.3 Monitoring & Auditing

Staff must be aware that there is capability and capacity for their actions within systems to be monitored, audited and recorded. The more sensitive the system, the more granular and extensive the monitoring and audits should be. The types of activities that can be monitored and audited are:

- Checking user lists and roles for each system to identify any changes
- Date and time a user account has been accessed
- When records are viewed with a system processing personal data
- Ensuring users accessing the system are the correct users
- Ensuring there has not been any inappropriate access by users who do have a right to view / access certain information

For each system, there should be an understanding of what events are monitored and how. Information regarding monitoring can be added to the asset register in the Information Asset Register.

Do not forget as well that individuals can request access to their personal information and request who has accessed their record. The audit trail details about such access can be made available upon such a request.

Any inappropriate access may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. In addition, unauthorised access of PCD is an offence and could lead to criminal prosecution.

<u>Confidentiality Audits</u>

The IG Team also undertake regular confidentiality audits to check compliance with data security such as locking computer / laptop screens when someone is away from their desk / ensuring confidential documents are stored securely. Results of these audits are reported to the Information Governance Board.

For further information, please see the Confidentiality Audit Procedure.

<u>Smartcards</u>

Smartcards are required to use and access IT systems essential to healthcare provision. Individuals are granted access to a Smartcard by the organisation's Registration Authority (RA). It is up to the organisation's RA Team to verify the identity of all healthcare staff that need to have access to PCD. Individuals are granted access based on their role and their level of involvement in patient care.

All staff issued with a Smartcard and passcode must be aware that they must comply with

the terms and conditions of issue. Failure to do so will be dealt with as a serious disciplinary matter.

Staff must not share or allow usage of their Smartcards by colleagues, including managers, peers or IT personnel, for any reason.

The use of Smartcards leaves an audit trail detailing access and usage, including only having viewed a record. This audit information may be used in disciplinary procedures regarding inappropriate or unauthorised access to systems.

For more information on Smartcards please refer to the organisations Registration Authority Policy.

6. DATA SECURITY STANDARD 5 – PROCESS REVIEWS

This standard states that,

This section provides guidance and links to further information on:

- Process checking / learning from incidents

6.1 Process checking / learning from incidents

The CCG need to ensure security breaches and near misses are recorded to identify and improve any problem processes, for example, staff not informing system administrators regarding change of roles which may change their access privileges on a system. They may continue to have access to information that they no longer require. The examples of processes to be checked are:

- New starters access rights – are these done in a timely fashion
- Temporary staff access rights – are these added and removed in a prompt way
- Revoking leavers access rights – are leavers accounts deleted in a timely fashion especially for those staff who are administrators
- Staff moving roles – ensure old role access is revoked especially if previous access was to personal data and is no longer required
- Storage and transfer of data – ensuring that staff save data on approved platforms only – do not use unauthorised cloud storage or sharing facilities
- Internet access and blocking – ensuring malicious website and inappropriate content are blocked but content has to be reviewed in the context of those viewing it. For example, if there is inflexibility and lack of granularity can lead to a situation where a pharmacist cannot access drug sites
- Initial boot and login times – ensuring these are not excessive waiting times to log on
- Locked down devices and business applications – ensuring that ports and applications are locked down

The above list is not exhaustive. The IG Team also undertake regular confidentiality / data security audits to check compliance with data security and confidentiality and make changes to processes to improve practices. We also learn from reported data security breaches / IG incidents to mitigate such events occurring in the future by putting in place relevant processes. A Data Protection Impact Assessment Proforma is also a process we use to check potential risks to the processing of personal data for a new project or change to a system / asset processing.

For further information, please see the Confidentiality Audit Procedure, the Data Security Breaches / IG Incident Policy and Procedure and the Data Protection Impact Assessment Proforma and Guidance.

7. DATA SECURITY STANDARD 6 – RESPONDING TO INCIDENTS

This standard states that,

This section provides guidance and links to further information on:

- Incident Reporting process for reporting data security breaches / IG incidents
- Anti-virus / Email security
- CareCERT alerts

7.1 Incident Reporting process for reporting data security breaches / IG incidents

The implementation of GDPR and DPA 2018 has brought with it a new regime around data security breaches / incident reporting. This creates two new obligations, the mandatory reporting of serious personal data breaches and the need to inform individuals when their rights and freedoms have been harmed.

All incidents are reported following the NHS Digital guidance called the "Guide to the Notification of Data Security and Protection Incidents".

https://www.dsptoolkit.nhs.uk/Help/29

Incidents are classified as defined in the Article 29 Working Party on Personal data following the CIA triad as per below:

- **Confidentiality** – unauthorised or accidental disclosure of, or access to personal data
- **Integrity** – unauthorised or accidental loss of access to, or destruction of, personal data
- **Availability** – unauthorised or accidental alteration of personal data

All data security breaches such as those listed below must be reported to the IG Team, following the CCG's incident reporting procedure, as soon as possible to ensure they are scored accordingly and reported within the mandatory timeframe. If you become subject to a cyber-attack or your IT equipment is compromised meaning you are unable to work, please also contact IT Service Helpdesk.

Examples of data security breaches (based on ICO classification) are:

- Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)
- Cyber incident (phishing / Denial of Service / key logging software / exfiltration & other cyber incidents)
- Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords
- Data left in insecure location
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact data
- Failure to use bcc when sending email to groups
- Information uploaded to webpage in error
- Insecure disposal of hardware
- Insecure disposal of paperwork
- Loss of theft of unencrypted device
- Loss or theft of only copy of unencrypted data
- Loss or theft of paperwork
- Verbal disclosure

Fines for personal data breaches can, in principle, be as high as 4% of the organisations turnover, or 20m Euros, whichever is higher. This is a massive increase from the £500,000 cap under the previous Data Protection Act 1998.

In addition organisations that fail to report an incident when they should have done can be further fined 2% of turnover or the equivalent of 10m Euros, whichever is higher.

The guidance and procedure states when the CCG must report an incident to the ICO. An organisation is permitted to notify the initial findings to the ICO and then provide additional information as the investigation progress.

For further detailed information, please see the Data Security Breaches / IG Incidents Reporting Procedure and the NHS Guidance "Guide to the Notification of Data Security and Protection Incidents." This must be read together.

Informing individuals

GDPR mandates that if the personal data breach has indeed harmed the rights and freedoms of an individual, the CCG must inform the individuals accordingly using clear and plain language, including:

- An explanation of what occurred
- Contact details for the DPO
- Possible consequences of the breach
- How the CCG has mitigated the breach

The IG Team will undertake this in conjunction with the DPO / SIRO and / or the Caldicott Guardian and the department where the incident occurred.

Staff must always:

- Report any Data Security (IG) incident of concern via following the procedure for reporting of data security breaches / IG incidents
- Think carefully before sharing PCD

It is better that a potential incident / breach is reported and discounted later, rather than not being reported and becoming more serious by not being known about.

Incidents are robustly investigated so that lessons can be learned from them, both within the team that it occurred and to benefit the organisation.

7.2 Anti-virus / Email security

Anti-virus products

The IT Services deploy suitable measures to reduce the likelihood of IT / cyber incidents by implementing anti-virus solutions. Each end point (e.g. computer / laptop / tablet) is protected by an anti-virus agent. This generates alerts every time an event occurs (such as a detected infected file). The system is then interrogated by IT Security from IT Services to know what they are, whether they are fixed by the anti-virus product or if further action is needed.

Email

The CCG use NHSMail exclusively to send and receive emails. This is managed and offers protection against infected files, mass mailing protection, secured access to logs and quarantined files for audit purposes, generic attachment filtering, email content and attachment inspection, controls to prevent the forwarding of infected emails and rules for which attachments can or cannot be sent. This solution states the volume of spam mails and emails being filtered.

For further information, please contact IT Services.

7.3 CareCERT alerts

IT Services are signed up to receive CareCERT alerts.

What is CareCERT?

NHS Digital has a Care Computer Emergency Response Team (CareCERT). The CareCERT Data Security Centre works to make sure patient data is used securely and safely, through the services, guidance and support they give to health and care organisations to respond effectively and safely to cyber security threats. This is because of the rising risk of cyber threat across all sectors. The CCG will benefit from the latest technological knowledge and world class guidance developed by experts

The IT Team act upon intelligence supplied by CareCERT. They provide a complete repository of threats and vulnerabilities to act on. It is important that these are acted upon as the implications of not doing so were seen apparent during the 12th May 2017 Wannacry cyber-attacks. Another example is a computer virus that affected the Northern

Lincolnshire and Goole NHS Trust in autumn 2016 for five days, meaning that thousands of routine operations and outpatient appointments had to be cancelled. This was because the virus caused the computer network to crash.

For further information regarding CareCERT, please click on the link below:

https://digital.nhs.uk/services/data-security-centre

8. DATA SECURITY STANDARD 7 – CONTINUITY PLANNING

This standard states that,

This section provides guidance and links to further information on:

- Continuity plan for data security incidents
- Roles and Responsibilities

8.1 Continuity plan for data security incidents

The CCG has a Business Continuity Policy and Plan which outlines what staff must do in the event of a data security incident such as a cyber attack or if there is an IT incident which prevents you from working. These are supported by the IT Services disaster recovery plans and processes to ensure the network / IT failure is fixed / corrected as soon as possible. The plan is tested to ensure it is fit for purpose.

8.2 Roles and Responsibilities

In the event of invoking the business continuity plan, it is essential that team members are able to get hold of contacts to assemble the response team. Therefore, there is a mandate that a hard copy of the contacts is kept securely and kept up to date. In some cases, a press release may be required and therefore draft press materials are available for when such occasions occur.

For further information, please see the Business Continuity Policy and Plan and you can ask your Resilience lead for further information.

As a member of staff, do you know or are aware of the business continuity plans in place for if and when a cyber-attack occurs. What are your department / team processes if you cannot access information on a system / online for a defined amount of time? How you will ensure that you can continue to provide a service?

9. DATA SECURITY STANDARD 8 – UNSUPPORTED SYSTEMS

This standard states that,

This section provides guidance and links to further information on:

- Knowing your software
- Security updates / patching

9.1 Knowing your software (unsupported and supported software)

Software, being digital, does not degrade over time however it does become unsupported and therefore potentially vulnerable. Dependent upon the software, this may cut-off until it is patched or upgraded. The ramifications of using software beyond its support date will vary but could be potentially dangerous as per the Wannacry cyber-attack in May 2017 which affected those systems which had not been updated.

The IT Services have a tool to provide an inventory of hardware assets and the software that resides on them. This will list the version number and when their end life is.

Supported versions of software are those which the manufacturer or IT services supports with patching and upgrades. End of life software is not update or patched and can be vulnerable to threats. The tool reports whether a patch or upgrade is required.

Unsupported software is categorised according to business risk and any data security risks are identified and managed by the IT Security Team. Where it is not possible to upgrade / update software, the reasons are identified and the SIRO confirms that the risks of using unsupported systems are being managed accordingly.

9.2 Security updates / patching

Security updates and patching are carried regularly out as per the Data Centre Server Patching Process held by IT Services. Desktop infrastructure is regularly updated with security updates and patching is performed daily to remote endpoints (desktops / laptops / tablets).

For further information, please contact IT Services.

10. DATA SECURITY STANDARD 9 – IT PROTECTION

This standard states that,

This section provides guidance and links to further information on:

- Network Security
- Penetration Testing for web applications and Plans
- Remote Working / Portable Devices
- The Privacy and Electronic Communications Regulations (PECR)

10.1 Network Security

Networking components are physical devices which are required for communication and interaction between devices on a computer network. They include (but are not limited to):

- Firewalls
- Switches and hubs
- Bridges
- Routers
- Wireless devices

These devices often have the same username and password and thus these must be changed to ensure the devices are not vulnerable.

In order to maintain network security, the IT Services Team carry out the following:

- Ensure that all networking components have had the default password changed to increase security
- Restricting the installation of potentially suspicious files;
- Regularly updating computers to protect against system vulnerabilities;
- Ensuring computers are routinely monitored for viruses, and that anti-virus software is in place;
- Having an email filtering system to “catch” suspicious emails before they reach the end user;
- Protecting the network borders with firewalls to restrict access;
- Only allowing the use of encrypted memory sticks.

To support this, all staff must:

- Never share usernames / passwords with anyone, including line managers and IT;
- Update their passwords regularly and keep them complex by using a combination of upper and lower case letters, numbers, and special characters (such as question marks and exclamation marks);

- Never subscribe to non-work related email subscriptions with work email account;
- Not follow links or open attachments from an unrecognised sender;
- Ensure any changes to your IT systems are only completed with IT authorisation;
- Ensure they report any suspicious incidents or faults to IT immediately

Due to the nature and sensitivity of the IT Network Security Policy produced by the IT Services, it is not published.

10.2 Penetration Testing and Plans

Penetration testing is a systematic process of probing for vulnerabilities in applications and the network. The IT Services undertake penetration tests at least annually and the scope and results of which include the SIRO. Once the test is complete, an improvement plan needs to be put in place to outline the top risks which are discussed by senior management. Testing is a continuous cycle of improvement following the PDCA (Plan, Do, Check and Act) model.

10.3 Remote Working and Portable Devices

Today's working environment offers flexible working patterns which mean there are far more staff working remotely or mobile. Although these working practices are advantageous, it is important for users to understand the associated risks, and ensure that information accessed remotely or held on portable devices, is protected by adequate security.

Staff are responsible for the security of any portable devices issued to them, and should take all necessary precautions to avoid loss, theft or damage. Should this occur it should be reported to the IT Services and to your line manager at the earliest opportunity.

<u>Remote Working and Portable Devices Best Practice Guidance</u>

- Encryption is mandatory for all organisation issued mobile devices
- Any portable computing device is an attractive item and must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it ensure that it is safely stored out of sight
- You must not leave the device unattended for any reason unless the session is 'locked' and it is in a safe working place, devices must not be left in an unattended publically accessible room
- Ensure that other non-authorised users are not given access to the device or the data it contains.

<u>USB / Portable Computing Devices</u>

- All USB / portable computing devices, including memory sticks, must be obtained from IT Services and are encrypted – no other devices are to be used
- USB / portable devices should only be used to store personal confidential data when other more secure methods are not available;
- Information must not be stored permanently on portable devices. Always transfer documents back to a secure network storage area as soon as possible;
- You must ensure that any suspected or actual breaches of security are reported via

the IT Services

- Staff leaving the organisation or no longer requiring use of an organisation's procured device must return the device to their line manager;
- You should not under any circumstances use any mobile device whilst in control of a vehicle without an approved hands free kit;
- You must retain an awareness of your surroundings when using a mobile device, especially when discussing confidential information.

Destruction and Wiping of Removable Media / IT Equipment

If you have removable media including USB memory sticks requiring destruction, they must be returned to the IT Services for professional wiping and / or destruction.

For further information, please see the IT Equipment Disposal and Re-use Management Policy created by the IT Services.

10.4 The Privacy and Electronic Communications Regulations (PECR)

The Privacy and Electronic Communications Regulations (PECR) 2003 and sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications. The EU is in the process of replacing the e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR. However, the new Regulation is not yet agreed. For now, PECR continues to apply alongside the GDPR. PECR covers the areas below of which some are not applicable to the CCG:

- Marketing by electronic means, including marketing calls, texts, emails and faxes. This does not apply to the CCG.
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service. The CCG's website supplier needs to ensure compliance with this.
- Security of public electronic communications services. The CCG IT Supplier ensures the network and communications services are secure.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (e.g. caller ID and call return), and directory listings. The CCG IT Supplier ensures the network and communications services are secure but some of the items listed above will not apply such as itemised billing and line identification services.

PECR have been amended seven times and the latest version came into effect on the 9th January 2019. The more recent changes were made in 2018, to ban cold-calling of claims management services and to introduce director liability for serious breaches of the marketing rules; and in 2019 to ban cold-calling of pensions schemes in certain circumstances.

The GDPR does not replace PECR, although it changes the underlying definition of consent. Existing PECR rules continue to apply, but using the new GDPR standard of consent. This means that when the CCG use cookies or similar technologies on the website, from 25 May 2018, they must comply with both PECR and the GDPR.

Naturally, there is some overlap, given that both aim to protect people's privacy.

Complying with PECR will help you comply with the GDPR, and vice versa – but there are some differences and you must make sure you comply with both.

In particular, it's important to realise that PECR apply even if you are not processing personal data. For example, many of the rules protect companies as well as individuals, and the marketing rules apply even if you cannot identify the person you are contacting.

For more information on your other data protection obligations, see our separate Guide to the GDPR.

For more information, please see the ICO website on the link below:

https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

11. DATA SECURITY STANDARD 10 – ACCOUNTABLE SUPPLIERS

This standard states that,

This section provides guidance and links to further information on:

- Know your suppliers / due diligence
- Contracts – GDPR compliance

11.1 Know your suppliers / due diligence

The CCG have a repository of IT suppliers and third party suppliers / providers / processors who provide a service and / or system to the CCG and process personal data. This repository lists the services delivered, contract information & duration and information about due diligence as regards compliance with data security legislation. GDPR mandates the CCG as a Data Controller to know and provide direction to suppliers / processors. They must only act on instruction of the CCG.

A review of the repository is undertaken annually to ensure compliance with data security legislation and the National Data Guardian Data Security standards which includes the following:

- Checking for ICO enforcement, decision notices, audit or advisories
- Checking the Data Protection Registration
- Checking compliance with the Data Security and Protection Toolkit or equivalent checklist (such as the IGA health and care GDPR checklist for suppliers https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
- Checking the contract in place is GDPR compliant and has a review date

11.2 Contracts – GDPR compliance

Article 28 of GDPR mandates that all contracts with third parties who process personal data must be compliance with this article. The NHS Standard Contract is to be used which details the GDPR clauses. This includes:

- only act on the written instructions of the controller (the CCG)
- ensure that people processing the data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- only engage sub-processors with the prior consent of the controller and under a written contract
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- assist the controller in meeting its GDPR obligations in relation to the security of

processing, the notification of personal data breaches and data protection impact assessments
- notify the controller without undue delay if it becomes aware of a breach of the personal data it is processing on behalf of the controller
- delete or return all personal data to the controller as requested at the end of the contract and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something that would infringe GDPR or DPA 2018

Where the NHS Standard clause is not used with a processor / supplier, a letter has been sent to suppliers from the CCG SIRO to confirm their GDPR compliance with a GDPR clause included for them to sign to provide assurance to the CCG that they meet GDPR standards.

12. DEFINITIONS / GLOSSARY OF TERMS / ACRONYMS

Personal Data
Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Special Categories of Personal Data
Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. These special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership;
- Health Data;
- Sexual life / sexual orientation;
- Genetic data – *introduced under GDPR;*
- Biometric data – *introduced under GDPR.*

Personal Confidential Data (PCD)
Personal data including any health related information (including where health related information can be derived from context) or health related information in a context from which personal data can be identified, is personal confidential data.

Anonymisation
This is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. GDPR does not apply to anonymised information.

Pseudonymisation
Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

DSPT
Data Security & Protection Toolkit. The new self-assessment tool provided by NHS Digital, formerly known as the IG Toolkit.

GDPR
General Data Protection Regulations

DPA 2018
Data Protection Act 2018

SIRO
Senior Information Risk Owner

DPO
Data Protection Officer

CIA
Confidentiality, Accountability, Integrity

IGA
Information Governance Alliance

PECR
This stands for the Privacy and Electronic Communications Regulations (PECR) and sits alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

Processing
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data Controller
This 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

Data Processor
This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Consent
Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal Data Breach
This means 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;

Health Data
This means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

ISS (Information Society Service)
Any service normally provided for remuneration, at a distance, by means of electronic

equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. Basically this means any online service that you sign up to such as Facebook / Twitter and where you can purchase online such as Amazon.