NHS
County Durham
Clinical Commissioning Group

Information Governance Handbook 2019-2021

12 May 2020

CONTENTS

1. INTRODUCTION

This handbook has been produced by the NECS Information Governance Team to provide staff with the necessary knowledge to comply with good Information Governance (IG), data protection legislation, and National and Local guidance.

All CCG staff, whether permanent, temporary, or contracted via a third party are responsible for good information governance and for ensuring compliance with IG policies, procedures, and legislation on a daily basis.

Whilst NECS IG Team are there to provide specialist advice on legislation and answer IG queries, it is for Managers, Information Asset Owners (IAOs), and Information Asset Administrators (IAAs) to promote good Information Governance and to ensure compliance by team members / colleagues in their own area.

It is important to remember that Information Governance is **everyone's** responsibility. You must protect any and all personal or protectively marked data you come into contact with during your employment with the CCG.

2. WHAT IS INFORMATION GOVERNANCE (IG)?

At a basic level, IG is simply the sound management of the information assets in an organisation. Any piece of information handled by an organisation is considered an 'information asset' and they can be physical (hard copy), and electronic.

At a more complex level, IG includes a full range of local and national policies, procedures, guidance, and legislation – all of which must be adhered to.

Generally speaking, organisations within the healthcare system using data for secondary purposes (i.e. for purposes other than the purpose for which the data was originally collected/created) must only use data that does not identify individual patients, unless they have the consent of the patient themselves or some other legal basis.

Information Governance is a framework for handling information in a professional, confidential and secure manner. Information assets or 'data' can be personal and relate to service users / employees, or they can be corporate (e.g. financial information).

Any organisation can establish a consistent and logical IG framework for employees to handle data through 4 main areas, which will be the basis of this handbook:

1. **LEGISLATION** – Laws and governing principles that determine how information assets must be handled.
2. **PEOPLE** – Roles within the organisation with specific responsibilities and training for overseeing certain aspects of information governance.
3. **POLICIES** – Local and national guidance, and best practice regarding all aspects of information governance (including Records Management, Retention, Data Handling, Risk Management, and Training)
4. **AUDIT** – Independent and self-assessment of an organisation's approaches to information / data protection and security.

The aim of IG is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal and corporate information by helping staff to practice good IG. This is supported by the organisation's *Governance Strategy.*

IG balances the use and security of information and helps the organisation to be legally compliant, transparent, and reduce risk when processing data. ‘Processing’ simply means doing anything with data (creating it, storing it, accessing it, deleting or destroying it, sharing it, sending and receiving it).

All staff have a duty of confidentiality regarding personal or protectively marked information. This is based on Data Protection and other laws. Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal action and significant fines for both yourself and the CCG.

IG - WHAT MUST YOU KNOW?

Information Governance is largely concerned with protecting data and whilst, the organisation ensures its corporate data is protectively marked, the processing of personal data is governed by the *Data Protection Principles* outlined in Article 5.1 of the General Data Protection Regulations (GDPR). You must know these principles:

1. Article 5.1 a) The processing of data must be lawful, fair, and transparent.
2. Article 5.1 b) The purposes of processing data must be specific, legitimate, and explicit.
3. Article 5.1 c) Processing of data must be adequate, relevant, and limited (only process personal data when absolutely necessary)
4. Article 5.1 d) Data processed must be accurate (including the provision of rectification if found to be inaccurate).
5. Article 5.1 e) Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Article 5.1 f) Data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

WHY?

Article 83(5) (a) of GDPR states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to 20 million Euros, or 4% of your total worldwide annual turnover, whichever is higher.

3. INFORMATION GOVERNANCE POLICIES

The organisation has a suite of IG Policies (listed below). All of the policies can be obtained via County Durham CCG's website:

www.countydurhamccg.nhs.uk

Hard copies can be obtained from:

Jill Mathewson, Head of Corporate Services

- Confidentiality and Data Protection Policy
- Data Quality Policy
- Information Access Policy
- Information Governance and Information Risk Policy
- Information Security Policy
- Records Management Policy and Strategy
- Email and Internet Acceptable Use Policy
- Social Media Policy
- Incident Reporting and Management Policy

IG POLICIES – WHAT MUST YOU KNOW?

As an employee of the CCG it is important to read the above policies to ensure you are aware of and understand your IG responsibilities.

WHY?

To reduce information risks, to ensure compliance with the law, and to be prepared for mandatory training and random IG audits that take place throughout the year.

4. DATA SECURITY & PROTECTION (DSP) TOOLKIT

The DSP Toolkit is an online performance framework hosted by NHS Digital. All Health providers who provide NHS services and Social Care service providers, commissioners and suppliers are required to carry out self-assessments of their compliance against a set of data security standards, of which there are ten:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

Each standard is underpinned by several mandatory assertions against which the CCG must provide evidence to be considered to have met data protection and security standards. Many of the things we are required to do in our day to day work (including mandatory training) under the umbrella of IG is in order to evidence one or more elements of the DSP Toolkit.

NECS IG Team help the CCG to compile the evidence for their DSP Toolkit which must be submitted by 31st March every year.

DSPT – WHAT MUST YOU KNOW?

The DSP Toolkit:

- Is a self-assessment piece of software mandated for use by NHS, social care, GPs, commercial third parties and other providers of NHS/healthcare-related services to self-audit their IG compliance.
- CCGs have a number of mandatory assertions to evidence each year.
- Is subject to both internal and external audit.
- Has reports available online showing whether each organisation is compliant.
- Supports the CCG in bidding for services or partnerships by demonstrating good IG practice within the organisation.

WHY?

The DSPT covers every aspect of data protection and security in the organisation and so your work will impact on its completion. You may even be asked to provide evidence for inclusion in the Toolkit.

5. INFORMATION GOVERNANCE TRAINING

All CCG staff complete the IG training, known as 'Data Security Awareness Level 1', via the e-learning for health (eLfH) site which can be accessed via this link: https://portal.e-lfh.org.uk/

This training is mandatory for all staff and is also a mandatory requirement of the DSP Toolkit mentioned above. The training is available 24/7 and therefore learning can fit around your existing commitments. You do not need to complete the course or a module in a single session; your progress will be saved and when you return to your learning you can pick up where you left off. The only stipulation is that the training must be completed between 1st April and 31st March **every** year.

To access the training you should follow the instructions below:

Select:	login using user name and password contained in the email from e-LfH
Select:	My e-learning
Select:	Data Security Awareness (NHSD)
Select:	NHS Data Security Awareness Level 1
Complete:	All modules within this course

The required pass mark for the mandatory training is 80%
If you have any queries regarding your training, please contact the IG Team via necsu.ig@nhs.net

IG TRAINING – WHAT MUST YOU KNOW?

Further training can be obtained from the NECS IG Team in the areas of:

- Data Protection Impact Assessments
- SIRO, Information Asset Owner, Information Asset Administrator training
- GDPR
- DSP Toolkits
- Data Sharing
- Any ad hoc training as required by the CCG.

6. CALDICOTT GUARDIANS

There is a UK Caldicott Guardian Council which is the national body for Caldicott Guardians, who are responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities that provide social services must have a Caldicott Guardian.

A Caldicott Guardian is a senior figure responsible for protecting the confidentiality of service user's health information and enables appropriate information sharing. The Caldicott Guardian has a strategic and advisory role which involves representing and championing IG requirements and issues at Board or management team level and at other levels where appropriate. The Caldicott Guardian is a member of the CCG Governing Body and works closely with the Senior Information Risk Owner (SIRO) and Governance Lead who are represented on that group.

Before you handle or disclose any confidential information you should use the Caldicott principles as a guide. The seven Caldicott principles are as follows:

- **1. Justify the purpose(s) for use of 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.

- **2. Don't use personal confidential data unless it is absolutely necessary**
  Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

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

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

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

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

- **7. The duty to share information can be as important as the duty to protect patient confidentiality**
  Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers.

  If you are still unsure on review of the Caldicott principles please contact your line manager or the NECS Information Governance Team on 0191 375 1769.

CALDICOTT GUARDIANS – WHAT MUST YOU KNOW?

Dr Ian Davidson is the Caldicott Guardian for County Durham CCG.

Ultimately, the Caldicott Guardian will make the final decision as to what, when and how personal identifiable information is used, received or sent within the CCG's.

7. THE NATIONAL DATA GUARDIAN

The National Data Guardian (NDG) for Health and Social Care is an independent, non-regulatory, advice giving body in England sponsored by the Department of Health and Social Care. The NDG advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.

They set the Leadership Obligations and Data Security Standards around which the DSP Toolkit is formed.

The UK Caldicott Guardian Council is a sub-group of the National Data Guardian Panel. The chair of the UKCG council sits on the NDG Panel.

NATIONAL DATA – WHAT MUST YOU KNOW?

You do not need to be an expert in data protection legislation, but everyone who works within the NHS and/or with personal or confidential data should be aware of:

- The Caldicott Principles
- The Data Protection Principles
- The Data Security Standards
- The General Duty of Confidentiality

Compliance with these key principles and standards is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of data protection legislation.

8. THE DATA PROTECTION OFFICER (DPO)

The GDPR introduced a duty for organisations to appoint a DPO if they are a public authority or body, or if they carry out certain types of data processing activities.

DPOs assist the organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (which for us is the Information Commissioner's Office (ICO)).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. This can be an existing employee or someone who is externally appointed.

In some cases several organisations can appoint a single DPO between them.

DPOs can help an organisation to demonstrate compliance with the law and are part of the enhanced focus on 'accountability'.

DPOs – WHAT MUST YOU KNOW?

It is important to know who your DPO is. The DPO for County Durham CCG is:

- Liane Cotterill – Senior Governance Manager at NECS. Liane.cotterill@nhs.net

Liane covers the DPO role for several CCGs and so by extension, the NECS IG Team can also offer the same DPO advice to staff if needed.

- NECSU.IG@nhs.net

9. SENIOR INFORMATION RISK OWNER (SIRO)

The Senior Information Risk Owner (SIRO) is accountable for, and acts as a champion in; managing information assets, the risks associated with them and any incidents surrounding them.

The SIRO will also ensure that the Executive Committee, Board (or equivalent) is kept up to date on all information risk issues. The role will be supported by the NECS Senior Governance Manager and the organisation's Caldicott Guardian, although ownership of the Information Risk programme will remain with the SIRO.

The main purpose of the SIRO role is as follows:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the organisation's information risk and incident management framework
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs

- Advising the Chief Executive or Board on the information risk aspects of the Annual Governance Statement

The SIRO would also be involved in the investigation of any data breach or serious incidents involving information and the subsequent mitigations put in place to prevent future occurrences.

SIROs – WHAT MUST YOU KNOW?

It is important to know who your SIRO is, especially if you are responsible for any information assets or think any information asset may be at risk. The SIRO for County Durham CCG is:

- Nicola Bailey

They must be informed of any identified risks to information governance or data security.

10. INFORMATION ASSET OWNERS (IAO) & INFORMATION ASSET ADMINISTRATORS (IAA)

The SIRO is supported by one or more IAOs (the number of IAOs in the organisation will depend on the number of information assets held).

The role of IAO is to understand what information is held and why, to add or remove information assets from the Information Asset Register, and to understand who has access (and why) in their own specific area.

They are therefore 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.

The NECS Information Governance Team will support the IAO(s) in fulfilling their role, which includes keeping a CCG Information Asset Register up to date.

An IAO may be involved in compiling responses to requests for information from the public such as Freedom of Information Request or Subject Access Requests.

Information Asset Administrators (IAAs) are also required to support the CCG’s SIRO and the IAO(s) and will work with the NECS Information Governance Team to ensure staff apply the Data Protection Act and Caldicott Principles within working practices.

INFORMATION ASSET OWNERSHIP – WHAT MUST YOU KNOW?

Information that has been held previously by NHS Durham Dales, Easington and Sedgefield CCG and NHS North Durham CCG is transferring to the new NHS County Durham CCG on 1 April 2020.

The Information Asset Owners (IAOs) and Administrators (IAAs) are as previously held for NHS DDES CCG and NHS North Durham CCG as follows. Information Asset Owners (IAOs) and Administrators (IAA) will be reviewed during quarter 1, 2020/21.

DDES CCG

Asset Area	Information Asset Owner (IAO)	Information Asset Administrator (IAA)
CCG Policies and Procedures	Jill Matthewson, Head of Corporate Services	Amy Heron, Administrator
ISFE (Finance and Ordering System)	Mark Booth, Head of Finance	Jackie Waldock, Finance Administrator
Business Continuity Plan	Jill Matthewson, Head of Corporate Services	Amy Heron, Administrator
CCG Governing Body and Committee Papers	Jill Matthewson, Head of Corporate Services	Mags Wells, Governance Administrator
Freedom of Information Requests	Jill Matthewson, Head of Corporate Services	Mags Wells, Governance Administrator
Complaints information	Jill Matthewson, Head of Corporate Services	Margaret Coyle, Executive Assistant
CCG Constitution	Jill Matthewson, Head of Corporate Services	Amy Heron, Administrator
HR Information	Jill Matthewson, Head of Corporate Services	Janet Walker, Team Admin
Finance Spreadsheets	Mark Booth, Head of Finance	Jackie Waldock, Finance Administrator
Commissioning Intentions	Sarah Burns, Director of Commissioning	Lorrae Rose, Commissioning Manager (NECS)
DDES CCG Website	Jill Matthewson, Head of Corporate Services	Gail Cobb, NECS Communications and Engagement Team
GP Teamnet	Jill Matthewson, Head of Corporate Services	Laura Kirkup, Commissioning Support Officer
Safeguarding Incident and Risk Management System (SIRMS)	To be agreed	To be agreed
DDES CCG Facebook	Jill Matthewson Head of Corporate Services	Gail Cobb, NECS Communications Team
Hardware including PCs, laptops, PDA and communication devices	Sarah Lambert, Head of Corporate Services	Susan Stewart, Receptionist Sharon Cockroft, Receptionist
North Durham CCG and DDES CCG Collaborative working shared folder	Jill Matthewson, Head of Corporate Services	Amanda /Million, Corporate Administrator

North Durham CCG

Asset Area	Information Asset Owner (IAO)	Information Asset Administrator (IAA)
Commissioning	Michael Houghton, Director of Commissioning and Development	Lisa West, Team Admin
Corporate Office	Jill Matthewson, Head of Corporate Services	Amanda Million, Corporate Administrator
Engagement	Joseph Chandy, Director of Primary Care	Sharon Gooch, Personal Assistant
Finance and Performance	Richard Henderson, Chief Finance Officer	Judith Hunter, Team Admin
Integration	Lesley Jeavons, Director of Integrated Community Services	Andrea Bell, Personal Assistant
Nursing and Quality	Gill Findley, Director of Nursing	Janet Walker, Team Admin
Practice Nurse Links	Pauline Lax, Practice Nurse Links	Amanda Million, Corporate Administrator
Primary Care	Joseph Chandy, Director of Primary Care	Sharon Gooch, Personal Assistant
Quality and Safety	Dr Ian Davidson, Medical Director	Judith Hunter, Team Admin
Safeguarding Children	Marie Baister, Designated Nurse, Safeguarding Children	Val Lowther, Team Admin
Safeguarding Adults	Sue Nuttall, Safeguarding Adults' Manager	Val Lowther, Team Admin

11. THE NECS IG TEAM

The NECS IG Team is the CCGs main source of IG advice. The team is made up of 6 people:

- 1 x Senior Governance Manager – Liane Cotterill
- 1 x Senior Governance Officer – Beverley Smith
- 4 x Information Governance Officers
    - Sophie Parker;
    - Paul Robert Atkinson;
    - Hilary Murphy; and
    - Pamela Coxon.

The main responsibilities of the NECS IG Team are as follows:

- Ensuring requests for information from the public (such as Freedom of Information Requests and Subject Access Requests) are logged and responded to.
- Providing IG advice and training to CCG staff
- Approving and advising on the completion of Data Protection Impact Assessments.
- The provision of a suite of CCG IG Policies and Procedures
- The provision of a Data Protection Officer service.
- Carrying out Confidentiality Audits at CCG premises and administering IG questionnaires to CCG staff.
- Ensuring the completion of the CCG's DSP Toolkit each year.

NECS IG TEAM – WHAT MUST YOU KNOW?

If you have an IG Query you can contact your assigned IG Officer here:

- Paul Atkinson (paulrobertatkinson@nhs.net)

Or the wider IG Team here:

- IG Mailbox – NECSU.IG@nhs.net

12. THE COMMON LAW DUTY OF CONFIDENTIALITY

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges and is also referred to as 'case law'. The law is applied by reference to previous cases and is said to be 'based on precedent'.

The general position is that, if someone provides information to you in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent or some other legal basis. In practice, this means that all personal information, whether held on paper, computer, visually, audio recording, or even held only in your own memory, must not be disclosed without a legal basis to do so.

All employees are responsible for maintaining the confidentiality of information gained or accessed during their employment, this also extends after they have left the employment of the CCG. This is not only a contractual requirement but a requirement of the Data Protection Act 2018.

Employees should also protect the confidentiality of information that is classed as Commercial in Confidence; this information should be treated with the same care as personal confidential information.

In order to provide assurance that access to confidential information is gained only by those individuals who have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

Monitoring should be carried out to ensure that irregularities regarding access to confidential information can be identified, reported to the senior management, and action taken to address the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

The NECS Information Governance Team will ensure that quarterly audits of security and access arrangements are conducted on a regular basis covering premises and work areas. The areas to be audited will include:

- Security applied to manual files e.g. storage in locked cabinets/locked rooms
- Arrangements for recording access to manual files, e.g. access requests by solicitors, police, data subjects etc.
- Evidence that checks have been carried out to ensure that person(s) requesting access have a legitimate right to do so
- The existence and location of noticeboards containing personal information
- The use of and disposal arrangements for post-it notes, notebooks and other temporary recording material
- Retention and disposal arrangements
- The location of fax machines and answer phones which receive confidential information (use of fax machines is not recommended due to the IG risks involved)
- Confidential information sent or received via email – e.g. security applied and e-mail system used
- Information removed from the workplace – e.g. authorisation gained either for long term or short term removal
- Security arrangements applied – e.g. transportation in secure containers
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information
- Security applied to laptops, compliance with the NECS Remote Access Policies
- Evidence of shared passwords being used within the area audited
- General physical security of premises where information is concerned.

Audits will be carried out by a series of staff IG questionnaires and observations / visits.

For further information please refer to the CCG's Confidentiality and Data Protection Policy and Confidentiality Audit Procedure.

DUTY OF CONFIDENTIALITY – WHAT MUST YOU KNOW?

Three circumstances making the disclosure of confidential information lawful are:

1. where the individual to whom the information relates has consented
2. where disclosure is necessary to safeguard the individual, or others, or is in the public interest
3. where there is a legal duty to do so, for example a court order or legal basis under the Data Protection Act.

No employee should never knowingly;

- breach their legal duty of confidentiality,
- allow others to do so, or
- breach any of the organisation's security systems or controls.

Knowingly misusing or failing to properly safeguard any 'confidential' data will be regarded as a disciplinary offence and, in some cases, a crime.

Confidentiality Audits will usually take place without you knowing and involved an IG Officer attending your workplace and making observations against set criteria. You can avoid having confidential information in the wrong place by applying a '6S' approach to your workspace:

- **"SORT"** remove unneeded items
- **"SET IN ORDER"** organise a place for everything
- **"SWEEP AND SHINE"** clean and inspect
- **"STANDARDISE"** make it consistent
- **"SUSTAIN"** keep it up
- **"SAFETY"** make safety a priority

If you are asked to complete a confidentiality Questionnaire, it will come to you in electronic format from the IG Team. Most of the answers to the questions can be found in local procedures, policies, or this handbook with a little research. Completed Questionnaires should be returned to the IG Team as soon as possible. You will be given feedback on any areas of improvement required.

13. TYPES OF DATA

There are many different types of information, several of which can be considered as confidential, personal, sensitive, or protectively marked in some way:

1. **Personal (non-sensitive)** – Personal data is information recorded about a living individual that enables them to be identified. In order to lawfully process personal data, you must identify a lawful basis for doing so under GDPR Article 6. Personal data includes the following examples:

✓ Name
✓ Date of birth
✓ Address
✓ Postcode
✓ Next of kin
✓ Carer's details
✓ National insurance number
✓ Bank details
✓ Unique identifier e.g. NHS number

2. **Personal (sensitive)** – Sensitive personal data (also known as 'special category data) is personal data which the GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis under GDPR Article 6 and a separate condition for processing special category data under GDPR Article 9. These do not have to be linked. Some examples of personal sensitive data are:

✓ Medical conditions
✓ Sexual orientation
✓ Religious beliefs
✓ Political views
✓ Ethnic origin
✓ Criminal convictions
✓ Trade union membership
✓ Genetic and biometric data

3. **Corporate** – Corporate information belongs to an organisation or company and can be considered 'sensitive' at a commercial level. A public authority's corporate information is less protected than a private company. This is due to their business and how it is run being publicly funded and therefore much of the information is publicly disclosable. Some examples include:

✓ Contract information
✓ Minutes of meetings
✓ Financial details

4. **Anonymised data –** Is personal or personal sensitive data than has been altered so that individuals can no longer be identified and it is virtually impossible to re-identify them. Anonymised data can be shared lawfully and where this might facilitate care it must be shared.

5. **Pseudonymised data** – Pseudonymisation takes the identifying fields within a data set and replaces them with artificial identifiers, or pseudonyms (such as a code or reference number). The purpose is to render the data record less identifying and therefore reduces concerns with data sharing and data retention. The difference between this and anonymised data is that individuals can still be identified by pseudonymised data if access to the re-identifying codes is provided.

PROCESSING DATA – WHAT MUST YOU KNOW?

Processing data simply means doing anything with it (storing, viewing, accessing, deleting etc.) and this is governed by several laws. Some of the key legal requirements for public organisations processing data that you need to be aware of are:

- Individuals whose data is being processed have a right to be informed about how and why and with whom it may be shared. We do this via our Fair Processing Notice (sometimes called a Privacy Notice or Privacy Statement) and every organisation processing personal data must publish one by law.

  www.countydurhamccg.nhs.uk

- It is a legal requirement to keep a register of every information asset the organisations holds. This is known as an Information Asset Register and records the type of data, its location, the legal basis under which the organisation holds it, who is responsible for it, and how long it will be retained. IARs must be kept up to date by adding any new information assets and removing ones that are no longer held. Each information asset will have an Information Asset Owner (IAO) who is responsible for maintaining that asset on the IAR.

- One of the governing principles of data protection is for data to be of good quality (meaning it is accurate, reliable, and useful). For more information on data quality see the Data Quality Policy.

14. INFORMATION GOVERNANCE INCIDENTS.

It is important that information remains safe and secure at all times. All staff are encouraged to report all Information Governance related incidents via the Safeguard Incident Reporting Management System (SIRMS). The CCG / NECS can then investigate and learn from those incidents.

Information Governance incidents are categorised as follows (this list is not exhaustive):

- Damage to hard copy records (fire, water)
- Inappropriate access to / disclosure of personal information
- Information left unattended) printer, empty office etc.)
- Lost / stolen equipment paper/hard copy (mobile, USB, laptop)
- Misdirected email received containing confidential information
- Misdirected email sent containing confidential information
- Misdirected hard copy received (e.g. post, fax, etc.)
- Misdirected hard copy sent (e.g. post, fax, etc.)
- Other (IG)
- Password sharing
- Smart card issues

Where any of the above occurs and personal information has been breached outside of the NHS family then the CCG has effectively lost control of that data and this would likely be considered a serious (i.e. Reportable to the ICO) Information Governance incident. If this occurs and you need advice about an incident please contact your line manager or a member of the Information Governance team whose contact details can be found on the final page of this handbook.

KNOW YOUR RESPONSIBILITIES:

The SIRMS system can be accessed by following the link below:
https://sirms.necsu.nhs.uk

Remember that serious (reportable) incidents where personal data has been breached outside of the NHS family must be reported to the ICO within 72 hours. NHS Digital Guidance can be found at the link below: https://www.dsptoolkit.nhs.uk/Help/29

The individuals affected must also be made aware. More information on this can be found on the ICO website. https://ico.org.uk/for-organisations/report-a-breach/ and from the CCG's Incident Reporting and Management Policy.

15. INFORMATION SECURITY AT WORK

Smartcards

- Treat your smart card as you would your bank card and keep it in a safe place.
- Never share your smartcard with anyone.
- Do not write down your password.
- Never leave your smartcard unattended or in the smartcard reader when not in use.
- Report the theft, loss or damage to your smartcard via the SIRMS system immediately to ensure that your card is cancelled / replaced as soon as possible.
- Read, understand and sign the declaration on your RA01 form to agree your responsibilities.
- Access to personal identifiable information through clinical systems should be for a legitimate reason, any other access will be viewed as a breach of confidentiality.

System / Account Passwords

- Passwords are not to be shared or used even under supervision in training situations.
- Ensure that strong passwords are used, i.e. using a minimum 8 digit combination of letters, numbers and special characters (!?£&%$ etc.).
- Do not use consecutive passwords i.e. mypassword1, my password2, my password 3 etc.
- Do not write passwords down where they can be easily found i.e. on a sticky note next to your workstation or on your laptop.
- Change passwords when prompted.

- Change passwords immediately if you suspect that they have been compromised and report the incident via SIRMS.
- Do not base your password on something that can be easily guessed such as your own name, make of car, car registration number, pet's name etc.
- Do not recycle old passwords.

Your Work Environment

- Ensure that filing cabinets containing confidential information are locked when not in use.
- Ensure that filing cabinets are not in areas accessible to members of the public / visitors.
- Always wear your identity badge.
- Whenever possible always escort on-site visitors.
- Do not take confidential information out of the office unless on approved business.
- Safeguard the security and confidentiality of information at all times, for example lock your workstation when away from your desk.
- If confidential information is taken off site by agreement do not leave them in your car in plain sight overnight; ensure that they are stored securely.
- If they must be left in a vehicle, ensure they are out of sight and the vehicle is locked.

Printing and Photocopying

- Photocopying machines should not be situated in areas to which visitors / members of the public have access.
- No documents should be left on or in the photocopier after copying.
- Photocopying should be taken away immediately after printing.
- When printing from a PC use the locked print option.

Confidential Waste

- Ensure that you dispose of confidential information appropriately in the confidential waste bins provided.
- Confidential waste bins should be kept locked at all times.
- The organisation's approved contractor is Shred-It, the contract is managed by NHS Property Services.

Eavesdropping

- Ensure that where conversations are conducted relating to organisational business either over the telephone, face to face or in the close proximity of public/reception areas, care must be taken that personal information is not overheard by persons who do not have a legitimate need to hear such information.
- This also applies where recorded messages are re-played.

Physical Measures

- Controlled entry to buildings.
- Out of hour's security.
- Visitor policy.
- ID badges must be visible at all times (for staff and visitors)**.**

Telephone Calls and Answering Machines

- Verify the details of the caller.
- Obtain their telephone number.
- Provide the minimum information necessary.
- If in doubt of the caller's identity tell the caller that you will ring back.
- When returning the call if possible use a phone number obtained from an independent source.
- Take care when making a phone call that you do not reveal confidential information by being overheard – make confidential phone calls in a separate room.
- If you must leave an answer phone message leave the minimum information necessary.
- Ensure that you replace the receiver correctly after leaving an answerphone message.
- Ensure that you listen to answer phone messages in an environment where they cannot be overheard.

Mobile Devices (Laptops, Tablets, Phones, Memory Sticks)

- Store work issued mobile equipment securely when not in use on and off site.
- Ensure files containing personal or confidential data are stored on the appropriate shared drive with controlled permissions (need-to-know access).
- Only use NECS approved encrypted memory sticks – available from the NECS IT Help Desk.
- Report any stolen work issued mobile equipment immediately via SIRMS: https://sirms.necsu.nhs.uk/ .
- Understand that the security of your work issued mobile equipment is your responsibility.
- When using a work mobile device you must ensure that it is safe to do so.
- Ensure that the information on the screen of a mobile device is not visible to anyone who is not authorised to see it.
- Never view confidential information in a public place where it can be seen by members of the public.
- Always lock your device when unattended. Hold down the Windows button and the 'L' button to lock a screen.
- When using a Wi-Fi connection, stick to using only HTTPS (secure) websites (this means your web browsing is encrypted even if it travels over an unencrypted connection). You can check if any web site is using HTTPS by looking for the small padlock by the address bar within your web browser.
- Use NHS provided remote access (VPN, Virtual Private Network) for work purposes when connected to any Wi-Fi; this means that all your network traffic (not just your web browsing) is encrypted.
- Do not Disable the virus protection software or bypass any other security measures put in place.
- Do not leave mobile equipment unattended in a public place e.g. hotel rooms, train luggage racks etc.
- Do not install or download software onto devices yourself. This should only ever be carried out by NECS IT Technician.

- Do not Connect to unsecured public Wi-Fi networks - these are often found in hotels, coffee shops and other public spaces. You can confirm if a network is secure when you see a small padlock next to it as you're selecting to potentially join the network.

INFORMATION SECURITY – WHAT MUST YOU KNOW?

Information is everywhere and in every possible format. You process it every day and some of it is incredibly sensitive and protected not only by local policy, but by UK Law. It is important to follow best practice and the advice of the IG team with regards to processing or controlling information for the CCG.

If you don't think you 'need' to see some information, then you probably shouldn't. Keeping the information you handle to only that which you need to know to do your job will ensure information incidents are kept to a minimum.

16. INFORMATION SHARING

IG should never be considered as a barrier to the appropriate sharing of information. For example, in 2013 a new Caldicott principle was added that promoted the principle 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 CGG must ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

Guidance on Information Sharing for Safeguarding Practitioners updated by the Department for Education in July 2018 has Seven Golden Rules of Information Sharing which are broadly applicable to all instances of sharing personal and sensitive data:

1. Remember that the GDPR, DPA18 and human rights law 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 (and/or their family where appropriate) 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, or your IG lead, 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 DPA18 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 (see principles).
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.

Staff sharing personal information with other agencies must be aware of the CCG's requirement to have a Data Sharing Agreement in place for the routine sharing of personal data.

Information sharing for non-care purposes

Information that is to be used or shared for non-care purposes, for the benefit of the community, should generally be anonymised. This 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 Data Protection legislation, 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 sharing the information. 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

INFORMATION SHARING – WHAT MUST YOU KNOW?

Sharing or Disclosing personal data can be a complex issue which will typically require expert advice and consideration. If data is not personal or protectively marked in anyway, then it can be shared and the rules on handling it are minimal.

Staff faced with decisions regarding the sharing of personal or personal sensitive data should have regard to national guidance and seek advice from the NECS IG Team if necessary.

Never share information if you are unsure whether you are legally allowed to do so. Always seek advice if in doubt.

17. SECURE SENDING OF INFORMATION

It is important to ensure data is kept secure whenever it is shared, transferred, or transported anywhere – especially outside of the NHS.

Email

- Staff must be careful when sending emails containing personal identifiable / commercially sensitive information via email.
- The minimum information should be sent via email.
- Both sender and recipient in NHS organisations must have an NHS mail account ending in @nhs.net.
- Organisations can get their email system accredited for security by NHS Digital therefore the landscape is constantly changing.
- Further information is available from NHS Digital here https://digital.nhs.uk/services/nhsmail/the-secure-email-standard
- Care should be taken to ensure that emails are sent / forwarded to the correct recipient.
- Emails should include an appropriate disclaimer:
- **CHECK** any attachments containing personal information before sending and then **CHECK AGAIN** or have someone else check. Most IG incidents that occur involve the wrong personal information being attached to an email or sent to the wrong place through human error.

Note the legacy local and central government email domains (gcsx.gov.uk, gsi.gov.uk and gsx.gov.uk) stopped being used and were switched off completely in March 2019, as all local and central government organisations migrated to using .gov.uk email addresses for all email communication as they adopted the government secure email standard.

SECURE SENDING – WHAT MUST YOU KNOW?

Where person identifiable / business sensitive information is required to be sent to an organisation that has no facility to set up a secure encrypted email address the NHS Mail encryption feature can be used:

In the subject field of the email, enter [secure]'before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment. Further instruction on how to use this feature is available in the NHS Digital document Encryption Guide for NHSmail Version 2.0, October 2016 or from the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net

For further information please refer to the CCG's Information Security Policy.

18. DATA PROTECTION LEGISLATION

The Data Protection Act 2018 defines UK law on the processing of identifiable data of living individuals. It is a piece of legislation which governs the protection of personal data in the UK. In practice it provides a way for living individuals to control the use of information about themselves.

The Act defines the data protection principles which are listed in Section 2 of this handbook:

The General Data Protection Regulations (GDPR) came into force on 25 May 2018 with the aim of establishing a single legislative regime for data protection across all EU member states. GDPR will apply in the UK whether we leave the EU or not because it has been established into UK Law via the Data Protection Act 2018. GDPR applies to all public authorities and any organisations processing personal data. The key changes to UK data protection law that the GDPR implemented are as follows:

- Introduction of a DPO
- There must be a consent process documented which has regard to the greater restrictions placed on the public sector.
- GDPR-compliant, binding contracts must in place with data processors and service providers.
- Data subjects are given much more control over their personal data under GDPR. Requests for personal data must be provided to a data subject within 30 calendar days of their request and we are not allowed to charge a fee. For more information see the Standard Operating Procedure – Subject Access Requests and Subject Rights Requests.
- The requirement to have a Fair Processing Notice / Privacy Notice.
- Requirement to keep a record of processing activities (via an Information Asset Register)

- Data Protection by Design & DPIA – organisations must consider data protection in all of its processing activities. Project and change management processes must be in place to actively embed Data Protection Impact Assessment (DPIA) processes. Existing PIA documentation will need to be amended to align with GDPR requirements to contain at least:
  - Systematic description of the processing activities and the purposes
  - Assessment of the necessity and proportionality of the processing
  - Assessment of the risk to the rights and freedoms of the data subjects
  - Measures to address the risks

LEGISLATION – WHAT MUST YOU KNOW?

You don't need to be an expert in the law, but you should at least be aware of the legislation and guidance surrounding IG that says how organisations must safeguard information, what processes are in place to use, secure, and transfer information, and how patients and the public have access to personal information. The CCG must comply with the following Laws and Regulations:

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- Data Protection Act 2018
- Freedom of Information Act 2000
- General Data Protection Regulations 2016
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Human Rights Act 1998
- Records Management Code of Practice for Health and Social Care 2016
- Information: To Share or not To Share (Caldicott2)
- Manual for Caldicott Guardians 2017
- Privacy and Electronic Communications Regulations

19. 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 here.

Staff can download leaflets, posters and other resources, including the poster to the left, 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 April 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.

NATIONAL DATA OPT OUT – WHAT MUST YOU KNOW?

> The national data opt-out replaces what were previously known as 'Type 2' opt-out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care. Any patient that had a Type 2 opt-out had it automatically converted to a national data opt-out from the launch date, and have received a letter with further information.

20. DATA QUALITY

Data quality is vital to the decision-making processes of any organisation. This is particularly important for a public service such as the NHS where financial integrity and public responsibilities of care need to be ingrained in the services provided.

Data Quality can be defined as captured information that is consistently fit for its intended use in representing real world figures and situations to help inform operational decision making and planning, risk assessment and financial transactions.

DATA QUALITY – WHAT MUST YOU KNOW?

The aim is for the CCG to hold the most accurate and up-to-date personal information and to make sure that the activity against individuals is recorded correctly.

A data subject has the legal right for the information you hold about them to be correct and accurate and to have this rectified if it is not.

For more information on Data Quality see the CCG's Data Quality Policy.

21. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

A DPIA is a tool used to identify and then reduce, eliminate or justify any potential risks to the security or confidentiality of personal data within a 'project'. A DPIA must be carried out at the beginning of any project which involves the collection and use of personal information / sensitive personal information. A DPIA can reduce the risk of harm to data subjects through the misuse of their personal information and ensures that there is a legal basis identified for every instance of processing personal data.

A 'project' could entail:

- The introduction of any new system (electronic or paper) or information technology.
- The introduction of any new service (clinical or non-clinical).
- Any change to the way in which staff collect, record, use, publish or share personal information about patients, staff or members of the public.
- A new policy or procedure.

For any 'project' where the processing of personal data is happening it is a legal requirement to conduct a Data Protection Impact Assessment. Even projects that do not include the processing of personal data should at least have a DPIA 'initial screening' to make sure. See section 19 below for more information.

More information can be found on DPIA and how to conduct them via the CCG's DPIA standard operating procedure. This also includes the DPIA Template.

The DPIA template can be accessed via the CCG's shared folder or from the NECS IG Team.

If you need any advice on a new project or a changing system or process and need help with the completion of a DPIA please contact the NECS Information Governance Team.

DPIAs – WHAT MUST YOU KNOW?

All processes involving the high risk processing of personal data must have a DPIA conducted to ensure risks or prevented, reduced, eliminated, or accepted.

Anything with an accepted risk that cannot be mitigated must be reported to the ICO. Speak to the NECS IG Team for more information if you think you have identified a risk that cannot be reduced or eliminated.

It is vital, and a legal requirement to conduct DPIAs as soon as possible and to always consider the impact on a person's privacy of anything you do or any knew process you introduce. This approach is known as 'Privacy by Design'.

22. DATA SUBJECT RIGHTS

A Data Subject is any living individual who can be identified by their personal data. If you handle a data subject’s personal data, that person has certain legal rights, which are as follows:

New Right to Restriction
The marking of stored data with the aim of limiting their processing in future. The CCG must be willing / able to respond to data subjects' extended right of restriction of processing where the accuracy of data is contested, processing is unlawful, is no longer needed except for defence of legal claims or where the data subject has objected to the processing pending verification whether the legitimate grounds of the controller override those of the data subject.

New Right to Erasure (right to be forgotten)
The CCG must be willing / able to respond to data subjects' extended right of erasure. Applies where; data is no longer necessary for the purpose, subject withdraws consent, subject objects, data have been unlawfully processed, to comply with a legal obligation, collected in relation to the offer of information society services to a child. There are exemptions (for example, medical history cannot be erased).

New Right to Data Portability
The CCG must be willing / able to respond to data subjects' extended right of data portability. Where processing is done by automated means a subject is allowed to receive his/her own data which he/she has provided to a controller in a structured, commonly used machine-readable format and to transmit it to another controller. Applies only where consent-based or for the performance of a contract.

Extended Right to Object
The CCG must be willing / able to respond to data subjects' extended right to object to processing. Applies where data is processed in the public interest or in the exercise of official authority vested in the controller or the legitimate interests of the controller; a subject may object but it is up to the controller to demonstrate that legitimate interests override the data subject’s right to object.

Extended Rights Regarding Automated Decision-making & Profiling
The CCG must be willing / able to respond to data subjects' extended rights in relation to automated processing and profiling. This is a right not to be subject to a decision based solely on automated processing, including profiling. Does not apply where necessary for a contract, is authorised by member state law or is based on the data subject’s explicit consent. Special categories (e.g. health) are excluded from automated decision-making or profiling unless there is explicit consent or substantial public interest.

Extended Right to Rectification
The CCG must be willing / able to respond to data subjects' extended right of rectification. This is a right to have inaccurate personal data rectified or have incomplete data completed.

DPIAs – WHAT MUST YOU KNOW?

A Fair Processing Notice (FPN) or Privacy Notice is a written statement that individuals are given when information about them is collected. The CCG's FPN will include:

- The CCG's identity
- The purpose(s) for which the CCG will process the information
- Any additional information in order to make processing fair and lawful
- An outline of the data subject's rights

The County Durham CCG's FPN for the public and service users can be accessed via the CCG website;

www.countydurhamccg.nhs.uk

A FPN relating to staff information is available on the CCG's intranet site via the link below:

https://teamnet.clarity.co.uk/Library/ViewItem/5972c3bf-c271-4c53-ba92-abb900b48469

23. 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 to their lifecycle to their eventual disposal. Any information held by the CCG is only of use if it can be retrieved easily and the data contained within it is accurate and up to date. Staff must feel confident that they know how to access and store information in order for them to carry out their role to the best of their ability.

Manual Records

Manual records when not in use should be stored securely. Confidential information should not be left lying around in accessible areas. When a record has become dormant consideration should be given to the CCG's Records Management Policy with regard to retention and disposal.

Electronic Records

Access to all PC's / laptops must be password protected. Passwords should not be shared. Computer screens should not be left on view for the public or staff to view personal or commercially sensitive information. PC's / laptops not in use should be locked by pressing Ctrl, Alt and Delete or logged out of completely.
Laptops and hand held devices must be kept secure in a safe environment. USB sticks must not be used for confidential information unless they are encrypted, password protected and approved by the NECS IT team.

Retention and Destruction of Records

Please refer to the retention periods in Annex Three of the IGA Records Management Code of Practice for Health and Social Care:
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

Where an information asset does not appear in Appendix three of the above Code of Practice then the default position is that records should not be kept longer than necessary for the original purpose for which they were collected.

Confidential records should be disposed of via the confidential waste bins provided.

RECORDS MANAGEMENT – WHAT MUST YOU KNOW?

The NECS IG Team can advise on how to manage records and can even arrange for the secure storage and retrieval of records via a third party supplier.

It is vital that every record / asset at the CCG is assigned an Information Asset Owner and appears on the Information Asset Register.

Any records that are to be boxed and stored / archived MUST but correctly indexed and their retention monitored.

Correct indexing means that the IAO knows which box contains which record so that it can be retrieved easily.

The IG Team DO NOT hold this information for you. It is the IAO's responsibility.

Any Records Management queries should be sent to the NECSU.RecordsManagement@nhs.net mailbox.

24. REQUESTS FOR INFORMATION FROM THE PUBLIC

Living individuals have a right under the Data Protection Act 2018 to access personal data about themselves which is held in either electronic or manual form by the organisation.

Subject Access Requests can be made by anyone at any time so it is very important that all staff recognise when a subject access request is being made. Within all applications for access to records the applicant will need to prove their identity.

When a Subject Access Request is received the organisation should acknowledge the request within 2 days and respond to the applicant within 30 calendar days. This can be extended by up to 60 further days if a request is particularly resource intensive or difficult. The clock only starts ticking on Subject Access Requests once the identity of the subject has been ascertained.

The Freedom of Information Act 2000 is an act of law and gives anyone the general right to request information from a public authority. Pubic authorities include government departments, local authorities, the NHS, councils, schools and police forces. Public authorities must also provide information that is freely available through an approved publication scheme. The CCG's publication scheme can be accessed by following the link below:

County Durham CCG – www.countydurhamccg.nhs.uk

A Freedom of Information request must be made in writing (or email) stating what information the applicant requires. The applicant does not have to state that it is a Freedom of Information request or a reason as to why they require the information and requests must be 'requester blind' meaning it does not matter who has made the request.

The law requires Newcastle Gateshead CCG to respond within **20 working days** of receipt and staff must ensure that FOI requests are passed on to the NECS FOI team promptly.

It is extremely important that whenever CCG staff are required to provide information as part of the FOI process, this information is provided as soon as possible and without undue delay. FOIs that are not responded to promptly can attract complaints from requesters to the ICO.

Freedom of Information guidance for employees / the public can be found on the CCG's website by following the link below:

www.countydurhamccg.nhs.uk

REQUESTS FOR INFORMATION – WHAT MUST YOU KNOW?

Subject Access Requests and Freedom of Information Requests will be dealt with by the IG Team within NECS. Standard operating procedures as set out by the NECS Information Governance Team should be followed.

If you receive a request for access to personal records, or any queries regarding information held by the CCG, the request/query should be immediately forwarded to the Information Governance Team within NECS who will ensure that the request is processed and responded to within the time frame specified by GDPR or the Freedom of Information Act.

25. KEY CONTACTS

CCG TEAM:

Nicola Bailey
nicola.bailey5@nhs.net
Chief Officer – Senior Information Risk Officer (SIRO)

Jill Matthewson
jill.matthewson@nhs.net
Head of Corporate Services

Amanda Million
amanda.million1@nhs.net
Corporate Governance Officer

NECS INFORMATION GOVERNANCE TEAM:

Liane Cotterill – 01642 745042
liane.cotterill@nhs.net
Senior Governance Manager – Data Protection Officer

Beverley Smith – 07423090459
Beverley.smith54@nhs.net ***Senior Governance Officer***

Pamela Coxon – 0191 3746051
p.coxon@nhs.net
Information Governance Officer
Sunderland CCG and South Tyneside CCG

Hilary Murphy – 0191 2172625

hilary.murphy2@nhs.net
Information Governance Officer
North Tyneside CCG and Northumberland CCG

Sophie Parker – 0191 691 3652
Sophie.parker13@nhs.net
Information Governance Officer
North Cumbria CCG and Newcastle Gateshead CCG

Paul Atkinson – 01642 745581
paulrobert.atkinson@nhs.net
Information Governance Officer
Tees Valley CCG and County Durham CCG
SIRMS CONTACT

Wendy Marley – 0191 3744157
wendy.marley@nhs.net
Senior Governance Officer (SIRMS)

Document Management:

Version	Release Date	Author	Update comments	Approval route/date
V1	2015	NECS IG/CCG		unknown
V2	2016	NECS IG/CCG	Slight updates made to ensure robust IG arrangements	Head of Corporate Services– December 2016
V3	2017	NECS IG/CCG	Updated to incorporate the new General Data Protection Regulation Guidance	Executive Committee – 27/2/18
V4	2018	NECS IG/CCG	Updated to incorporate DPA2018 and new DSP Toolkit requirements	Senior Governance Manager NECS – CCG Governance Leads
V5	2019	NECS IG/CCG	Update following CCG feedback.	Senior Governance Officer - NECS
V6	2020	NECS IG/CCG	Updated following changes to 2019/20 DSPT	Senior Governance Manager NECS – CCG Governance Leads
V7	2020	NECS	Updated following merger	CCG Governance Leads