North Tyneside
Clinical Commissioning Group

Information Governance Staff Handbook and Code of Conduct

Contents

1. INTRODUCTION

This handbook has been produced to provide staff with the necessary information in order to comply with information governance legislation and national and local guidance.
All staff whether permanent, temporary or contracted are responsible for ensuring that they comply with Information Governance requirements on a daily basis.
Managers and Information Asset Owners (IAOs) and Administrators (IAAs) are responsible for promoting Information Governance and ensuring compliance by team members / colleagues.
Please remember that Information Governance is **EVERYONE'S** responsibility.

2. INFORMATION GOVERNANCE

Information Governance provides a framework for handling information in a confidential and secure manner. Information can be personal and relate to service users / employees or corporate, for example, financial information. The Information Governance agenda encompasses legal obligations, national and local guidance and best practice. The aim of Information Governance is to demonstrate that NHS North Tyneside CCG can be trusted to maintain the confidentiality and security of personal and corporate information by helping staff to practice good Information Governance. This is supported by the NHS North Tyneside Information Governance Strategy.

3. GOVERNANCE POLICIES

All North Tyneside CCG Information Governance Policies are listed below. All North Tyneside CCG Information Governance policies can be obtained via the North Tyneside CCG GPTeamNet site via the link below:
https://portal.gpteamnet.co.uk/North%20Tyneside/Topics/View/Details/3bd2f33d-c4e0-46e5-a1ab-a6ce009e7baf
Hard copies can be obtained from the IG Lead – Irene Walker, Head of Governance.

North Tyneside CCG's Information Governance Policies are as follows:

- 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
  Associated policies are as follows:
- Internet Acceptable Use Policy
- Social Media Policy
- Incident Reporting & Management Policy

Please ensure that you read the above policies to make sure that you are aware of and understand your Information Governance responsibilities.
IGT 14.1-131 2a

hscic Health & Social Care Information Centre

4. INFORMATION GOVERNANCE TOOLKIT

The Information Governance Toolkit is an online performance framework hosted by NHS Digital. All Health and Social Care service providers, commissioners and suppliers are required to carry out self-assessments of their compliance against a set of requirements. For the CCG this includes:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance

- Clinical Information Assurance

The 2018/19 version will be renamed the Data Security and Protection Toolkit. Currently the IG Toolkit refers to requirements however in the new version they will be replaced by assertions. Ten standards will be included within the new Toolkit with a list of assertions attached to each standard.

5. INFORMATION GOVERNANCE TRAINING

The NHS Digital (formerly HSCIC) IG training tool was de-commissioned on 31st December 2016. As of 1st October 2017 all staff should complete their Information Governance training via the e-learning for health (eLfH) site which can be accessed via the link below:
https://portal.e-lfh.org.uk/
In order to access the Data Security Awareness 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 new training is available 24/7 and therefore learning can be 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.

For those staff in specialist roles, the associated training modules will not be released until phase 2 of the eLfH rollout and therefore interim workbooks are required to be completed by these staff as an interim measure.
The workbooks for completion by staff in specialist roles are detailed below:

Job Profile	Workbooks for Completion
Caldicott Guardian *Medical Director*	1. **The Role of the Caldicott Guardian Workbook** 2. *Access to Health Records Workbook*
SIRO Executive Director of Nursing & Chief Operating Officer	1. **Introduction to Risk Management for SIROs and IAOs Workbook**
Information Asset Owner (IAO) • *Chief Finance Officer*	1. **Introduction to Risk Management for SIROs and IAOs Workbook**

Job Profile	Workbooks for Completion
• *Executive Director of Nursing & Chief Operating Officer* • *Head of Governance* • *Head of Finance* • *CQI Manager*	
Information Asset Administrator (IAA) PA to Executive Director of Nursing & Chief Operating Officer	1. *Introduction to Risk Management for SIROs and IAOs Workbook*
Line Managers • *Chief Finance Officer* • *Executive Director of Nursing & Chief Operating Officer* • *Director of Contracting & Commissioning* • *Deputy Director of Nursing, Quality & Patient Safety* • *Head of Improvement & Development* • *Head of Governance* • *Head of Finance* • *CQI Manager* • *Head of Planning & Commissioning*	1. **Access to Health Records Workbook**

Workbooks in bold are mandatory and those in light print and italics are recommended and at the discretion of the line manager.
The materials consist of a workbook with an assessment at the end. Once completed the assessments must be sent to the Information Governance team for marking. The completed assessment should be sent to the email address necsu.ig@nhs.net

*Please note: You will only be contacted should you fail to reach the required pass mark of 80%

If you have any queries regarding your training, please contact the IG Team via necsu.ig@nhs.net

6. CALDICOTT GUARDIAN

Dr Ruth Evans is the Caldicott Guardian for North Tyneside CCG. A Caldicott Guardian is a senior figure responsible for protecting the confidentiality of service user / employee information and enabling appropriate information sharing. The Caldicott Guardian has a strategic and advisory role which involves representing and championing Information Governance requirements and issues at Board or management team level and at other levels where appropriate. The Caldicott Guardian is a member of the Governing Body and works closely with the Senior Information Risk Owner and Head of Governance who are represented on that group.

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

1. **Justify the purpose(s)**
   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 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 of 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 3742767. Ultimately the Caldicott Guardian will make the final decision as to what, when and how the person identifiable information is used and received / sent by North Tyneside CCG.

The National Data Guardian completed a review of data security in 2016, resulting in the following recommendations:

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, provided through the revised Information Governance Toolkit.
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.

IGT 14.1-230 1a

7. CONFIDENTIALITY

Confidentiality relates to the duty to maintain confidence and respect a person's privacy. Privacy relates to personal information that a person would not wish others to know without consent for the information to be shared.

All employees are responsible for maintaining the confidentiality of information gained during their employment, this also extends after they have left the employment of North Tyneside CCG. This is not only a contractual requirement but also a requirement of the Data Protection Act with respect to person confidential information. 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 person confidential information.

No employee shall breach their legal duty of confidentiality, allow other to do so or breach any of the organisation's security systems or controls.

The Health and Social Care (Safety and Quality) Act 2015 introduces a new legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. This information is in the form of a single identifier, the NHS number. Health and adult social care commissioners and providers, including those contracted to provide services, need to consider the circumstances where information can be lawfully shared and the information that might facilitate the provision of health services and adult social care. There are several different types of information:

1. **Personal** – Personal information is information recorded about an individual that enables them to be identified. It can include one or more of 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. **Sensitive Personal (DPA 1998)** – Sensitive personal information relates to areas where prejudices can prevail, for example:

- ✓ Medical conditions
- ✓ Sexual orientation
- ✓ Religious beliefs
- ✓ Political views
- ✓ Ethnic origin
- ✓ Criminal convictions
- ✓ Trade union membership

3. **Corporate** – Corporate information belongs to an organisation or company, for example:

- ✓ Contracts
- ✓ Minutes of meetings
- ✓ Finance details

Effectively anonymised information can be shared lawfully and so where this might facilitate care it must be shared. Where information is associated with an identifiable individual (personal information) then the individual concerned should be informed about the proposed sharing for it to be lawful. Where the information is confidential personal information it is also necessary to have the individual's consent or some other legal basis for meeting the requirements of confidentiality law. In either case, an individual's objection to the proposed sharing should normally be respected.

7.1 Confidentiality Audits

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 Caldicott Guardian and action taken to address the situation, either through disciplinary action, the implementation or additional controls or other remedial action as necessary. Actual or potential breaches of confidentiality should be reported to the NECS Information Governance Team immediately, in order that action can be taken to prevent further breaches taking place.

The NECS Information Governance Team will ensure that audits of security and access arrangements are conducted on a regular basis. 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. tracking cards, access requests by solicitors, police, data subjects etc.

- Evidence that checks have been carried out to ensure that the person requesting access has 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 – e.g. safe haven faxes
- 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

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

For further information please refer to the North Tyneside CCG Confidentiality and Data Protection Policy & Confidentiality Audit Procedure
IGT 14.1-133 1c & 2b & 13-231 1b & 13-232 1b & 235 1c

8. SENIOR INFORMATION RISK OWNER

Dr. Lesley Young-Murphy, Executive Director of Nursing & Transformation is the Senior Information Risk Owner (SIRO) for North Tyneside CCG. The SIRO is accountable for the organisation 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 Quality & Safety Committee and Governing Body are 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.
IGT 14.1-345 1a

9. INFORMATION ASSET OWNERS

The SIRO is supported by an IAO. The role of IAO is to understand what information is held, what is added and what is removed, who has access and why 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 the assets. The NECS Information Governance Team will support the IAO / IAOs in fulfilling their role.

10. INFORMATION ASSET ADMINISTRATORS

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

The Information Asset Owners (IAOs) and Administrators (IAAs) within North Tyneside CCG are as follows:

Role	Name
Finance	
Information Asset Owner (IAO)	Jeff Goldthorpe
Information Asset Administrator (IAA)	Susan Askew
Ops & Commissioning	
Information Asset Owner (IAO) Information Asset Owner (IAO)	Anya Paradis
Information Asset Administrator (IAA) Information Asst Administrator (IAA)	Susan Askew
Administration	
Information Asset Owner (IAO)	Lesley Young-Murphy
Information Asset Administrator (IAA)	Susan Askew
Safeguarding	
Information Asset Owner (IAO)	Maureen Grieveson
Information Asset Administrator (IAA)	Susan Askew

11. INFORMATION SECURITY

11.1 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.

11.2 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
- 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, pets name etc.
- Do not recycle old passwords

11.3 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.
- If confidential information is taken off site by agreement do not leave them in your car overnight; ensure that they are stored securely.

11.4 Printing and Photocopying

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

11.5 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).

11.6 Eavesdropping

- Ensure that where conversations are conducted relating to organisation 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 right or need to hear such information.
- This also applies where recorded messages are re-played.

11.7 Physical Measures

- Controlled entry to buildings
- Out of hour's security
- Visitor policy
- ID badges must be visible at all times

11.8 Faxing Information

- Only use a fax machine if absolutely necessary
- The fax machine should be located in a secure environment
- The room which the fax machine is in should be locked when the room is left unattended
- The chance of misdialling will be minimised by pre-programming frequently used numbers
- Pre-programmed numbers should be checked for any updates or amendments on a regular basis
- Always let the recipient know that you are sending a fax and ask for confirmation of receipt

11.9 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.
- 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

11.10 Mobile Devices

The following devices are considered to be mobile devices:

- Laptops
- iPads
- Memory sticks
- Mobile/smart phones

When using an authorised work mobile device you must ensure that it is safe to do so:

- Ensure that the information on the screen is not visible to anyone not authorised to see it.
- Never view confidential information in a public place where it can be seen by members of the public.

Don't share your work mobile devices

- Work issued mobile devices should not be shared with anyone

When using a Wi-Fi connection

- Stick to using only HTTPS (secure) websites so that 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
- If possible, try not to 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

You should ensure you DO:

- 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
- Only use NECS approved encrypted memory sticks
- 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

You should ensure you DO NOT:

- Disable the virus protection software or bypass any other security measures put in place
- Leave work issued mobile equipment unattended in a car or visible when traveling between locations

- Leave mobile equipment unattended in a public place e.g. hotel rooms, train luggage racks etc.
- Install or download software

11.11 Communication via Text

- Ensure that the recipient has consented to receive text communication
- Ensure that the mobile number is that of the intended recipient
- Ensure that the content of the message contains the minimum information possible and will not breach confidentiality or contain material that the person may find embarrassing or damaging

11.12 Communication via Post

- Confirm the name, department and address of the recipient
- Seal the information in a robust envelope, ensure it is correctly addressed (do not use abbreviations) and mark as private and confidential where appropriate
- Add a return to address to the back of the envelope
- Where necessary ask the recipient to confirm receipt

11.13 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
- An email sent from an NHS mail account to the following email addresses are secure
    - @gcsx.gov.uk
    - @gsx.gov.uk
    - @pnn.gov.uk
    - @mod.uk
    - @pnn.police.uk
    - @gsi.gov.uk
    - @gse.gov.uk
    - @scn.gov.uk
    - @cjsm.net
- Care should be taken to ensure that emails are sent / forwarded to the correct recipient
- Emails should include an appropriate disclaimer

*Please note: 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 the word [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 North Tyneside CCG Information Security Policy
IGT 14.1-231 1b

12. INFORMATION GOVERNANCE INCIDENTS

It is important that information remains safe, secure and confidential at all times. All staff are encouraged to report all Information Governance related incidents via the SIRMS system. The CCG / NECS can then investigate and learn from those incidents.

Information Governance incidents are categorised as follows:

- Confidential/sensitive email received from external sender
- Confidential/sensitive email sent by NECS
- Confidential/sensitive info – unauthorised access/disclosure
- Confidential/sensitive info uploaded to website in error
- Confidential/sensitive paperwork – non-secure disposal
- Confidential/sensitive paperwork from external sender
- Confidential/sensitive paperwork lost/stolen
- Confidential/sensitive paperwork sent by NECS
- Confidential/sensitive information unattended (printer, office)
- Corruption or inability to recover electronic data
- Damage to hard copy records (fire, water)
- Inappropriate access to system/folder (actual/potential)
- Lost/stolen equipment (inc. mobile, USB, laptop)
- Non-secure disposal of hardware
- Other
- Password sharing
- Smartcard issues

If a serious Information Governance incident occurs or 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.

The SIRMS system can be accessed by following the link below:
http://10.97.194.139/safeguard/

Please note that low risk incidents (impact score 1 – 3) should be closed within 5 days and high risk incidents (impact score 4 – 5) should be closed down within 1 month.
IGT 14.1-349 2b

13. INTRODUCING A NEW PROCESS OR SYSTEM

The '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

For any 'project' the following considerations should be made with regard to Information Governance:

Confidentiality – does the project involve collecting / recording / processing / storing of person identifiable information (patients or staff)? If yes a Privacy Impact Assessment is required.
Consent – Is the consent of the individual required in order to collect / process / share their information? If you are unsure please contact the Caldicott Guardian or the NECS Information Governance team for advice.
Transfer of Information – Please use the 7 Caldicott Principles as a guide before transferring information.
Storing electronic information – Please ensure that information is held securely and backed up regularly.
Records Management – All records, either paper or electronic should be stored in an appropriate place and procedures for tracking, archiving and destroying records should be agreed.
Training – Consider what training staff will require before delivering the new process or using the new system.
Lifecycle of the Project – Consider how the information will be stored / archived / destroyed at the end of the project. Please refer to the Records Management Code of Practice for Health & Social Care 2016:
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

14. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) is a tool used to identify and reduce the privacy risks within a 'project'. A PIA must be carried out at the beginning of any project which involves the collection and use of personal information / sensitive personal information. A PIA can reduce the risk of harm to patients / staff through the misuse of their personal information.

A template PIA can be accessed via:

https://portal.gpteamnet.co.uk/Library/ViewItem/6cc1af41-2250-4c10-99d3-a6d400bbf5fe

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

*Please note that when the General Data Protection Regulation (GDPR) comes into force on 25 May 2018 a Privacy Impact Assessment (PIA) will be known as a Data Protection Impact Assessment (DPIA). Please see section 18.13 for further information.

For further information please refer to the North Tyneside CCG Information Security Policy
IGT 14.1-237 2a

15. FAIR PROCESSING NOTICE (FPN)

A Fair Processing Notice (FPN) is an oral or written statement that individuals are given when information about them is collected. A fair processing notice should 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

CCG's FPN for the public and service users can be accessed via the link below:

http://www.southtynesideccg.nhs.uk/fair-processing-notice/

*Please note that when the General data Protection Regulation (GDPR) comes into force on 25 May 2018 the CCG'S FPN will be called a Privacy Notice and will be required to included further information – please see section 18.11

A FPN relating to staff information is available on the CCG's intranet site via the link below: http://www.northtynesideccg.nhs.uk

IGT 14.1-250 1a

16. 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 North Tyneside 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.

16.1 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 North Tyneside CCG Records Management Policy & Strategy with regard to retention and disposal.

16.2 Electronic Records

Access to all PCs / 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. PCs / laptops not in use should be locked by pressing Ctrl, Alt & 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.

16.3 Retention and Destruction of Records

Records should not be kept longer than necessary. Please refer to the Records Management Code of Practice for Health & Social Care 2016 by following the link below:
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

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

For further information please refer to the North Tyneside CCG Records Management Policy and Strategy.
IGT 14.1-420 1b

DATA PROTECTION ACT 1998

17. DATA PROTECTION ACT 1998

The Data Protection Act 1998 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 8 data protection principles which are listed below:

1. Personal data shall be **processed fairly and lawfully** and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further **processed** in any manner incompatible with that or those **specified purposes**.
3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.
4. Personal data shall be **accurate** and, where necessary, kept **up to date**.
5. Personal data processed for any purpose or purposes shall **not be kept** for **longer than is necessary** for that purpose or those purposes.
6. Personal data shall be **processed in accordance with the rights of data subjects** under this Act.
7. Personal data must be kept **secure**. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall **not be transferred** to a country or territory **outside the European Economic Area (EEA)** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

18. GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 with the aim of establishing a single legislative regime for data protection across all EU member states. The government will implement GDPR through the Data Protection Bill, which will replace the Data Protection Act 1998. GDPR applies to public authorities and is concerned with the processing of personal data. The key implications are detailed below:

18.1 Data Protection Officer

A DPO must be appointed. May be a staff member of the data controller or the processor or may be fulfilled on the basis of a service contract. Must possess in-depth knowledge of data protection/GDPR, be adequately resourced and have clear reporting lines to the most senior management in the organisation. The DPO is an advisory role, not a decision-making role and conflicts of interest must be taken into consideration when appointing. The DPO must be contactable by data subjects.

18.2 Consent Process

There must be a consent process documented which has regard to the greater restrictions placed on the public sector with regard to its use. The controller must be able to demonstrate that the data subject has given consent to the processing operation. New rules exist where the consent

condition is relied upon and the data subject is a child. The CCG will need to be able to obtain and record consent to gather children's data.

18.3 Contracts

GDPR-compliant, binding contracts must in place with data processors and service providers. Controller /processor contracts must stipulate the following:

- Nature of the processing
- Act only on instruction of the data controller
- Confidentiality commitments
- Security measures
- Assist controller with subject rights, security and risk assessment
- Delete or return all personal data to the controller

18.4 Changes to Right of Access

Information must be provided to a data subject within one month and there is no fee unless the request is manifestly unreasonable - changes to local procedures, e.g. Subject Access Request procedure, will need to be made and communicated to involved parties/processor.

18.5 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.

18.6 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.

18.7 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.

18.8 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.

18.9 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 (eg health) are excluded from automated decision-making or profiling unless there is explicit consent or substantial public interest.

18.10 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.

18.11 Fair Processing/Privacy Notices

The CCG FPN already includes elements of what is required under GDPR. There are differences according to whether the data has been collected from the data subject or is from another source. A combined list of what must be included is provided below:

- Identity and contact details of the data controller
- Contact details of DPO
- Purpose of processing
- Legitimate interests pursued by the DC
- Recipients of data
- Details where data is transferred to a third country, where applicable
- Categories of personal data processed
- Sources of the data
- Retention period of the data
- Right to request access, rectification, erasure, restriction, objection, portability
- Right to withdraw consent
- Right to lodge a complaint with the ICO
- Existence of automated decision-making, including profiling

NB: Privacy Notices must be written in language understandable by children (defined in GDPR as 16 or under). The UK Data Protection Bill specifies an age no lower than 13.

18.12 Record of Processing Activities

A record of processing activities by controllers must be in place covering:

- Name and contact details of the controller and DPO
- Purposes

- Categories of data subjects and personal data
- Recipients of the data
- Details where data is transferred to a third country, where applicable
- Envisaged time limits for erasure, where possible
- Technical and organisational security measures
- A record of processing activities by processors must be in place covering:
- Name and contact details of the processor and DPO
- Categories of processing carried out on behalf of each controller
- Details where data is transferred to a third country, where applicable
- Technical and organisational security measures

This could be maintained in the form of an Information Asset Register, including mapping of personal data flows.

18.13 Data Protection by Design & DPIA

The CCG must be able to 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

18.14 Incident Reporting

Personal data breaches are to be reported by the controller to the ICO within 72 hours after becoming aware, unless the breach is unlikely to result in a risk to the rights and freedoms of a person. Information to be provided will be at least; the nature of the breach, how many people affected, categories of data, name and contact details of the DPO, likely consequences, measures and mitigating actions. Policies and procedures will need to be amended to reflect GDPR requirements.

A controller must notify a data subject without delay about a breach of their personal data where the breach is likely to result in a high risk to the rights and freedoms of the data subject.

18.15 Policies

Existing IG policies will be re-written to take account of GDPR. Non-IG policies which reference the DPA 1998 will need to be amended in line with GDPR.

19. SUBJECT ACCESS REQUESTS

Living individuals have a right under the Data Protection Act 1998 to access personal data about themselves which is held in either electronic or manual form by the organisation. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 (except for records relating to deceased patients). This type of request is known as a Subject Access Request.
All Subject Access Requests must be made in writing. 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 respond to the applicant within 40 calendar days.

All Subject Access Requests will be dealt with by the Information Governance 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 records, or any queries regarding access to records, 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 the relevant Act.

Please note that when GDPR comes into force on 25 May 2018 the following will apply with regard to the processing of subject access requests;

- The statutory timescale for compliance will reduce from 40 calendar days to 1 month
- Requests can be made free of charge. A "reasonable fee" can only be charged for further copies of the same information or where a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.
- Where an applicant has provided their personal data in a commonly used machine-readable format they are entitled to receive such information in this format on submission of a valid subject access request
- The response letter sent to an applicant is required to include the right to lodge a complaint with the 'supervisory authority' i.e. The Information Commissioner's Office (ICO).

For further information please refer to the North Tyneside CCG Information Access Policy and Subject Access Request Procedure
IGT 14.1-234 1b

20. FREEDOM OF INFORMATION ACT 2000

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 North Tyneside CCG publication scheme can be accessed by following the link below:
http://www.northtynesideccg.nhs.uk/contact-us/freedom-of-information/publication-scheme/

A Freedom of Information request must be made in writing (or email) stating what information they 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.

The law requires North Tyneside 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.

Freedom of Information guidance for employees / the public can be found on the North Tyneside CCG website by following the link below:
http://www.northtynesideccg.nhs.uk/contact-us/freedom-of-information/

For further information please refer to the North Tyneside CCG Information Access Policy

21. BUSINESS CONTINUITY

North Tyneside CCG has a Business Continuity Plan (BCP) which describes how the CCG will discharge its functions in the event of a major incident that causes serious interruption of business operations.

Business Interruption can be defined as;
'An unwanted incident which threatens personnel, buildings, operational procedures, or the reputation of the organization, which requires special measures to be taken to restore things back to normal'

The four key areas considered are:

- Damage/denial of access to premises;
- Non availability of key staff;
- Loss or damage to other resources;
- Loss/damage to IT or data.

To perform its duty on a day-to-day basis, North Tyneside CCG depends upon a wide range of complex systems and resources, and seeks to maintain a good reputation. Inevitably, there is potential for significant interruption to normal business or damage to the organisation's reputation through loss of those systems and resources. NTCCGs priorities when faced with a significant interruption (whether actual or impending) will always be to:

- Ensure the safety and welfare of its personnel and visitors;
- Endeavour to meet its obligations under legislative requirements;

- Secure replacement critical infrastructure and facilities;
- Protect its reputation;
- Minimise the exposure to its financial and reputational position;
- Facilitate a return to normal operations as soon as practicable.

The Head of Governance is the person with senior level responsibility for Business Continuity Management. Formal oversight of the CCG Business Continuity Management arrangements is the responsibility of the Governing Body supported by the Quality & Safety Committee.

For further information please refer to the North Tyneside CCG Business Continuity Plan
IGT 14.1-346 2c

22. THE INFORMATION COMMISSIONER

The role of the Information Commissioner is to ensure compliance with the Data Protection Act, the Freedom of Information Act and the Environmental Information Regulations. The Information Commissioner's Office has the power to levy substantial fines up to £500,000 and in some cases initiate court proceedings on both organisations and individuals. Please see below some examples of monetary penalties:

Linda Reeves
4 September 2017
A former data co-ordinator employed by The University Hospitals of North Midlands NHS Trust has been prosecuted at North Staffordshire Magistrates' Court. Linda Reeves accessed the sensitive medical records of colleagues as well as people she knew that lived in her locality, without the consent of the data controller. Ms Reeves pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £700, ordered to pay costs of £364.08 and a £70 Victim Surcharge.

Brioney Woolfe
11 August 2017
A former employee of Colchester Hospital University NHS Foundation Trust, Brioney Woolfe, has been prosecuted at The Colchester Magistrates' Court. The former Midwifery Assistant pleaded guilty to two offences under section 55 of the Data Protection Act for accessing the sensitive health records of friends and people she knew and disclosing some of the personal information obtained. Ms Woolfe was fined £400 for the offence of obtaining personal data and £650 for disclosing it. Ms Woolfe was ordered to pay prosecution costs of £600 and a victim surcharge £65.

HCA International Ltd.
28 February 2017
The Information Commissioner's Office (ICO) has fined a private health company, HCA International Ltd, for failing to keep fertility patients' personal information secure.

The £200,000 monetary penalty has been issued as a result of an ICO investigation into the way the Lister Hospital was transferring, transcribing and storing records of IVF appointments.

The London hospital is part of a worldwide network of private health care facilities offering a range of services including fertility treatment. The issue was uncovered in April 2015 when a patient found that transcripts including details from interviews with Lister Hospital IVF patients could be freely accessed by searching online.

The investigation revealed the hospital had been routinely sending unencrypted audio records of the interviews by email to a company in India since 2009. Details of private conversations between a doctor and various hospital patients wishing to undertake fertility treatment were transcribed in India and then sent back to the hospital.

The ICO found the Indian company could not restrict access to the personal information because it stored audio files and transcripts using an unsecure server.

HCA International breached the Data Protection Act 1998 by failing to ensure that their sub-contractor acted responsibly.

The General Data Protection Regulation (GDPR), the new data protection law coming into force in the UK in May 2018, will strengthen the ICO's powers to fine companies. Fines of up to four per cent of a company's global turnover could be issued where a serious breach of data protection law has occurred.

Whitehead Nursing Group
25 August 2016

A nursing home in County Antrim has been fined £15,000 for breaking the law by not looking after the sensitive personal details in its care.

The nursing home issued an unencrypted laptop to a member of staff who took their laptop home. The bag was left in the employee's living room. The home was burgled during the night and the laptop stolen. The burglary was reported to the police but the laptop has still not been recovered.

The laptop held confidential (and sensitive) personal data relating to 29 residents of the nursing home including their name, date of birth, mental and physical health and 'do not attempt to resuscitate' status. The laptop also held confidential (and sensitive) personal data relating to 46 staff at the nursing home. The employee regularly took her laptop home to complete outstanding work.

The nursing home did not have any policies governing the use of encryption, homeworking and the storage of mobile devices or provide any training on data security for its employees.

The General Data Protection Regulation (GDPR), the new data protection law coming into force in the UK in May 2018, will strengthen the ICO's powers to fine

companies. Fines of up to four per cent of a company's global turnover could be issued where a serious breach of data protection law has occurred.

Regal Chambers Surgery
11 August 2016
A GP practice that revealed confidential details about a woman and her family to her estranged ex-partner has been fined £40,000 by the Information Commissioner. The woman warned the Practice of the family's 'problems' and asked the Practice not to inform her ex-partner of her whereabouts.

The estranged ex-partner submitted a subject access request regarding their child. The child's records were sent to the ex-partner 4 days after receipt of the request. The records contained sensitive and confidential data including the telephone contact details for the child's mother, her parents and the elder child of whom the ex-partner was not the father. It also included a number of child protection reports compiled by the Police and correspondence with Social Services.

The General Data Protection Regulation (GDPR), the new data protection law coming into force in the UK in May 2018, will strengthen the ICO's powers to fine companies. Fines of up to four per cent of a company's global turnover could be issued where a serious breach of data protection law has occurred.

23. THE INFORMATION GOVERNANCE TEAM

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

Joanne Appleby – 0191 3742767
joanne.appleby1@nhs.net
Senior Governance Officer (IG)
Sunderland & South Tyneside CCGs

David Cull – 0191 3746051
d.cull@nhs.net
Information Governance Officer
Newcastle Gateshead & Darlington CCGs

Hilary Murphy – 0191 2172625
hilary.murphy2@nhs.net
Information Governance Officer
North Tyneside & Northumberland CCGs

Kieran Williams – 0191 3751761
kieran.williams@nhs.net
Information Governance Officer
North Durham & DDES CCGs

Paul Atkinson – 01642 745581
paulrobert.atkinson@nhs.net
Information Governance Officer
Hartlepool & Stockton & South Tees CCGs

SIRMS CONTACT

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

24. INFORMATION GOVERNANCE STAFF HANDBOOK AND CODE OF CONDUCT CONFIRMATION SLIP

I confirm that:

I have received my copy of the Information Governance Staff Handbook and Code of Conduct and I understand my Information Governance responsibilities.

Name ……
Signature……..
Job Title……
Workplace……
Date……..

Please tick the boxes below to confirm that you have read and understood the following Information Governance policies and procedures:

☐ 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 Acceptable Use Policy
☐ Social Media Policy
☐ Incident Reporting & Management Policy
☐ Confidentiality Audit Procedure
☐ Subject Access Request Procedure
☐ Information Labelling and Classification Procedure
☐ Information Asset Management Procedure
☐ Privacy Impact Assessment Guidance

***Please note:** North Tyneside CCG's procedures are available on GPTeamNet

Please return to:

Information Governance Team
NHS North of England Commissioning Support Unit
Information Governance Office
John Snow House
Durham University Science Park
Durham
DH1 3YG

Alternatively please email this slip to:

NECSU.IG@nhs.net