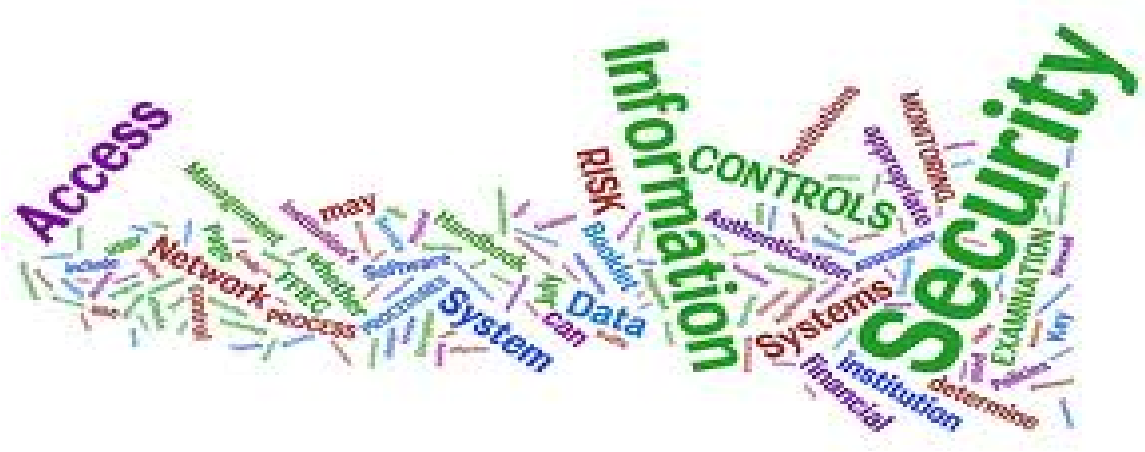
NHS
Mansfield and Ashfield
Clinical Commissioning Group

NHS
Newark and Sherwood
Clinical Commissioning Group

Information Governance Staff Handbook



August 2014
Version 2

Document History

Document Reference:	IG42
Document Purpose:	The document compliments all other Information Governance policies and supports awareness requirements for information governance in the CCG
Date Approved:	August 2014
Approving Committee:	Information Governance Management and Technology Committee
Version Number:	2.0
Status:	FINAL
Next Revision Due:	August 2015
Developed by:	Information Governance Services, Greater East Midlands Commissioning Support Unit (GEM CSU)
Policy Sponsor:	Director of Outcomes and Information, Nottinghamshire CCGs
Target Audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to lay members, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit

Revision History

Version	Revision date	Summary of Changes
1.0	August 2013	Revised in line with NHS England Policies and updated to reflect version 11 of the Information Governance Toolkit
1.1	May 2014	Revised in line to reflect Version 12 of the Information Governance Toolkit
1.2	August 2014	Further revisions following comments from GEM CSU IG Product Group.
2.0	September 2014	Approved at IG Management and Technology Committee

Document Dissemination Information

Reference Number	Title	Available from
IG	Information Governance Staff Handbook	CCGs publication scheme

Contents

What is Information Governance?

Information Governance (IG) allows organisations and individuals to ensure that personal confidential information is handled legally, securely, efficiently and effectively, It additionally enables organisations to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for information and assist compliance with Corporate Governance standards.

This handbook has been produced to provide staff with the necessary information required to comply with Information Governance requirements, relevant legislation and organisational policies and procedures.

What do You need to know about Information Governance?

Information Governance is a framework used across every NHS organisation and every staff member must make sure they understand their own personal responsibilities.
Everyone that manages sensitive personal or confidential information (this includes information relating to patients and staff) must be aware of the following:

- The importance of the information held
- The legislation, guidelines and best practice for managing important information
- Why individual responsibility must be taken for how records are obtained, recorded, used, kept and shared information

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis. Managers are also responsible for promoting IG standards and ensuring compliance with team members (especially where they have direct contact with NHS organisations). Wherever possible all staff should complete mandatory IG training appropriate to their role in their first week of employment.

Information Governance provides a consistent way for employees to deal with the different standards and legislation that apply to information handling, including:

- The Data Protection Act 1998.
- The Freedom of Information Act 2000
- The common law duty of confidence
- The Caldicott Principles
- The NHS Information Governance Toolkit
- The NHS Social Care Record Guarantee
- The Confidentiality NHS Code of Practice
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice

Information Governance Toolkit

The Information Governance Toolkit (IGTK) is a self-assessment tool which NHS organisations and their partner agencies are required to complete on an annual basis. The IGTK is developed and maintained by the Health and Social Care Information Centre (HSCIC) and provides a standard for information governance requirements for the NHS. The IGTK requires organisations to assess themselves against requirements for:

- management structures and responsibilities, including staff training
- confidentiality and data protection
- information security

The organisation is audited annually against the IGTK compliance to ensure that information is managed correctly, and that it is protected against unauthorised access, loss, damage and destruction. If the organisation is found to be non-compliant it is compelled to put processes in place to remedy the deficit. The organisation is required to be at Level 2 compliance to ensure that it can give assurances to the public and stakeholders that the NHS and its partners can be trusted with personal data.

All staff are required to complete mandatory annual IG Training as part of the IGTK, and staff with specific roles, such as access to sensitive or personal information, need to complete additional training appropriate to their role.

Information Governance Training

Information Governance training is mandatory for all staff and must be completed each year. All staff, including temporary, contract and lay staff, need to complete a basic Information Governance module at the start of their employment. If a role has access to personal confidential data, sensitive or corporate data then additional modules will need to be completed. Specific additional training is required for Senior Information Risk Owners (SIROs), Caldicott Guardians and for Information Asset Owners (IAOs). Training needs analyses will be completed by line managers on induction to ensure that training appropriate to staff roles is completed.

Information Governance Training via Electronic Staff Record

The HSCIC has developed an online training tool (IGTT) in order to ensure staff have consistent and comprehensive training available. There are a number of modules available depending on type of organisation and staff roles within it. The learning includes and assessment of understanding for each module.

CCG substantive staff are required to complete their mandatory IG training via the Electronic Staff Record (ESR). ESR is a portal to the IG Training Tool but records the completion of the module within ESR instead of in IGTT.

New staff need to complete the Introduction to Information Governance module, and may complete the Refresher module the following year.

ESR staff login can be accessed at the following link:
https://esr.mhapp.nhs.uk/OA_HTML/RF.jsp?function_id=30696&resp_id=-1&resp_appl_id=-1&security_group_id=0&lang_code=US&params=9Zy-Gm-ktVI4mxv1oNG.0Q&oas=AnCLzygo9rp01_JX6tr8-w

Staff should ensure that they follow the directions for accessing and completing a module as noted in the ESR user guide to ensure that the result is registered on ESR. A copy of the certificate can be printed as training record keeping.

Information Governance Training Tool

The Health and Social Care Information Centre provides an online Information Governance Training Tool (IGTT) which can be accessed at the following link:
https://www.igtt.hscic.gov.uk/igte/index.cfm

Users need to register under their organisation to ensure reports can be run bythe IGTT administrator. Staff who are not on substantive contracts, such as agency, contract or lay staff will need to complete their IG training via the IGTT as they do not have access to ESR. All staff who have had additional IG modules identified in their Training Needs Analysis will need to complete them on the IGTT and keep their own record of their training.
Users will need to input their local CCG organisational code.

What is Confidentiality?

A duty of confidence is in place where one person discloses information to another, eg patient to clinician, in circumstances where is it reasonable to expect that the information will be held in confidence.

How do you maintain confidentiality?

The confidentiality of information relating to individuals is protected through a number of measures:

- Procedures to ensure that all staff, contractors etc are at all times fully aware of their responsibilities regarding confidentiality.
- Gaining appropriate consent to process the information
- Recording information accurately and confidentially
- Keeping information private
- Keeping information physically secure
- Disclosing and using information with appropriate care

Maintaining Confidentiality – What individuals need to be aware of

Individuals must be made aware that the information they give may be recorded, may be shared in order to provide them with a service, and may be used to support audit activities and other work to monitor the quality of service that is being provided.
Staff should consider whether individuals would be surprised to learn that their information was being used in a particular way – if so, they are not being effectively told what they need to know.

Breaches in Confidentiality

Any breach of confidence, security incident, near miss or data loss can result in major consequences both for the staff member concerned, and the organisation, but mostly for people to whom the information relates (staff, patients or other members of the public).

Serious data losses can result in loss of public confidence and could lead to legal action being taken against the organisation. Whilst at a local level, it is possible that disciplinary action may be taken against staff for failure to comply with responsibilities in accordance with organisation policies. Staff should remember that deliberately looking at records or information without the necessary authority to do so, discussing personal details in inappropriate situations or with someone that does not need to know the details, or failing to follow organisation policy in transferring or using personal information could all lead to disciplinary action being considered.

For further information CCG policies are available on the publication scheme:

- **M&A**
- **N&S**

Confidentiality Audits

The NHS Care Records Guarantee requires that all organisations handling NHS information put in place mechanisms to ensure confidential information is protected. This requires access to confidential information to be monitored and audited locally, and in particular requires that there are agreed procedures for investigating confidentiality events.

Organisations should have processes to highlight actual or potential confidentiality breaches in their systems, particularly where personal confidential data (PCD) is held. They should also have procedures in place to evaluate the effectiveness of the controls within the systems.

All Clinical Commissioning Groups (CCGs) should already have control mechanisms in place to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints and alerts. A Confidentiality Audit Procedure has been developed which can be used to audit confidentiality and security within the CCG systems or at particular locations, in specified services or where a potential information breach has been identified.

All staff members with the potential to access confidential personal information should be aware that monitoring and auditing of access is carried out.

Failure by any employee to adhere to the organisational policy and its guidelines will be viewed as a serious matter and may result in disciplinary action.

Clinical Commissioning Groups and Access to Personal Confidential Data

Following the introduction of the Health and Social Care Act 2012 on 1 April 2014, Clinical Commissioning Groups (CCGs) no longer have a right to access personal confidential data (PCD) in the same way that Primary Care Trusts did.

CCGs can only access PCD if there is a legal basis for processing it, such as direct patient care requirement or there is explicit consent to do so. If you think that a service requires access to PCD, the IG Lead can advise to ensure that the requirement is legal. The need for access to, and storage of, PCD should be regularly reviewed to ensure the requirement is still relevant and that the agreed processes are being adhered to.

NHS England has secured temporary support under Section 251 of the NHS Act 2006 for commissioners to enable appropriate and long term solutions to be developed and implemented. This enables CCGs to:

- Transfer data from HSCIC to commissioning organisations' Accredited Safe Havens (ASHs)
- Enable CSUs and CCGs to undertake invoice validation within Controlled Environments for Finance (CefFs)
- Allow the disclosure of commissioning data sets (CDS) and GP data for risk stratification purposes and data processors working on behalf of GPs – under strict processing conditions.

For further information regarding information governance and the Health and Social Care Act follow the link below:

http://systems.hscic.gov.uk/infogov

Data Flow Mapping

Data Flow Mapping (DFM) is an exercise which is undertaken and reviewed by the organisation throughout the year with the aim of documenting all routine flows of information that are sensitive, either corporate sensitive information or data flows that contain personal confidential data (PCD). 'Routine' includes any scheduled annual data flows. Data Flow Mapping is a requirement of the organisation's Information Governance Toolkit and supports the assurance that the organisation can give to its stakeholders and third party contractors that it is compliant with NHS Information Governance standards.

The DFM exercise enables the organisation to check which data flows are in place, ensure that they are secure, and that there is a legal basis for the data flow. The DFM looks at all data coming into and going out of the organisation. It also documents the methods for transfer of data such as email, fax, post, courier, text message or from portable media which includes memory sticks, and mobile phones.

Occasionally a data flow will be identified that does not originate or terminate in a secure area or may be at risk of interception in transit. These data flows are noted as 'at risk' data flows and if no other method for transfer can be identified, the data flow is noted on the corporate risk register. If a more secure method can be found then the risk for that data flow is reduced.

Identified risks are reviewed by the Senior Information Risk Owner (SIRO) in conjunction with the GEM CSU IG Lead in order to determine any mitigating actions or whether a corporate risk should be raised.

Staff may be asked to assist with data flow mapping and to identify data flows that involve their team or department. If staff are unsure about any part of the process that they are being asked to participate in, they need to contact the CCG DFM lead or the CCG Information Governance lead.

What is the Data Protection Act 1998?

The Data Protection Act 1998 controls how personal information is used by organisations, businesses or the government. It sets standards which must be satisfied when processing data, which may include obtaining, recording, holding, using, or disposing of personal data.

The DPA sets out eight principles:

Principle 1: 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.

Principle 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 purpose or those purposes.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7: 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.

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

The Information Commissioners Office

The Information Commissioners Office (ICO) is the UK's independent official body set up to uphold information rights. The ICO promotes good practice, rules on complaints, provides information to individuals and organisations, and takes appropriate action when the law is broken.

The Information Commissioner is appointed by the Queen and is responsible for administering the provisions of the Data Protection Act 1998, the Freedom of Information Act 2000, the Privacy and Electronic Communications Regulations 2003, the Environmental Information Regulations 2004, and the INSPIRE Regulations 2009.

What the ICO does

The ICO has the power to issue monetary penalty notices up to £500,000 for serious breaches of the Data Protection Act and the Privacy and Electronic Communications Regulations. The ICO also monitors public authority compliance with the Freedom of Information Act and the Environmental Information Regulations. It is able to issue enforcement notices requiring organisations to comply with the law.

Many of the enforcement notices and fines are associated with the seventh principle of the Data Protection Act which relates to security of personal data.

Other Key Roles in Data Protection

Data Controller
A person who (either alone or jointly or in common with other persons) determines the purposes and the manner in which any personal data are, or are to be, processed.

Data Processor
In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject
An individual who is the subject of personal data.

Subject Access Requests

Under the Data Protection Act 1998 people (data subjects) can access their own personal data through a written request to the organisation holding their information (data controller). This includes information from medical records to HR records or any other information an organisation holds about the data subject. This applies to any organisation holding personal data, not just the NHS.

There are exemptions that may apply to releasing information and include circumstances where the release of the information may cause serious harm to the physical or mental health of the person or where information could be disclosed relating to, or provided by, a third person who has not consented to the disclosure.

If a Subject Access Request is received, it should be passed on to the Information Governance lead as soon as possible. The request must be responded to within 40 calendar days. It is up to the Information Governance lead or person managing Subject Access Requests to determine the identity of the applicant and if any exemptions apply.

Subject Access Request
Information Governance
Greater East Midlands Commissioning Support Unit
Birch House
Ransom Wood Business Park
Southwell Road West
Mansfield
Nottinghamshire
NG21 0HJ

Email: ignorth@gemcsu.nhs.uk

If a request is received for the medical records of a deceased person the request must immediately be passed on to:

Subject Access Request
Information Governance
Greater East Midlands Commissioning Support Unit
Birch House
Ransom Wood Business Park
Southwell Road West
Mansfield
Nottinghamshire
NG21 0HJ

Email: ignorth@gemcsu.nhs.uk

For further information CCG policies are available on the publication scheme:

- M&A

- N&S

Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) allows any person to contact a Public Authority to request information. The intention is to make Public Authorities transparent and open.

Anyone can ask in writing for any information held by the organisation, such as financial information, contract information, policies, reports etc. The information must be released providing the information is not exempt from disclosure. A range of exemptions include personal or confidential data, information which is commercially confidential or information which is already published and available elsewhere.

Key Points to Assist with FOI

- A request does not have to state that it is an FOI request. If in doubt forward to the FOI lead.
- All FOI requests are to be directed to the Communications/Freedom of Information team at the following email address:

Please send your request to FOI.Notts@gemcsu.nhs.uk. Or by post to:

Freedom of Information Officer
Greater East Midlands Commissioning Support Unit
Scarsdale
Newbold Road
Chesterfield
Derbyshire
S41 7PF

- Unless covered by an exemption under the Act, all records held by the organisation are affected, including diaries, notebook, emails and minutes from meetings

For further information on Freedom of Information click here:

http://ico.org.uk/for_organisations/freedom_of_information

What is Caldicott?

The Caldicott Committee (chaired by Dame Fiona Caldicott) made a number of recommendations in 1997 and a review in 2013 aimed at improving the way the NHS handles and protects patient information. All NHS staff must comply with the Caldicott principles set out below.

The Seven Caldicott Principles:

Principle 1 Justify the purpose(s) of using confidential information
Principle 2 Don't use personal confidential data unless it is absolutely necessary
Principle 3 Use the minimum necessary personal confidential data
Principle 4 Access to personal confidential data should be on a strict need-to-know basis
Principle 5 Everyone with access to personal confidential data should be aware of their responsibilities
Principle 6 Comply with the law
Principle 7 The duty to share information can be as important as the duty to protect patient confidentiality

What is a Caldicott Guardian?

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

Each NHS organisation is required to have a Caldicott Guardian. The Caldicott Guardian plays a key role in ensuring that NHS, councils with social services responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall Information Governance Framework.

M&A CCG – Dean.Temple@GP-C84051.nhs.uk
N&S CCG – Ei-Cheng.Chui@gp-c84037.nhs.uk

What is a Senior Information Risk Owner?

The role of a Senior Information Risk Owner (SIRO) should be undertaken by an Executive or Senior Manager on the Board or Executive Group and should be familiar with information risk management and the organisation's strategy for risk. The SIRO provides the board with assurance and is accountable to the CCG Chief Officer .

The NHS SIRO is responsible for ensuring organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist.

M&A and N&S SIRO - Elaine.Moss@newarkandsherwoodccg.nhs.uk
M&A and N&S deputy SIRO - Simon.Crowther@mansfieldandashfieldccg.nhs.uk

The SIROs key responsibilities

- **Leading and fostering** a corporate culture that values, protects and uses information for the success of the organisation and benefit of its patients
- **Owning** the organisation's overall information risk policy and risk assessment process and ensuring they are implemented consistently by Information Asset Owners (IAOs)
- **Advising** the Chief Executive or relevant accounting officer on the information risk aspects of the organisation's statement on internal controls.
- **Owning** the organisation's information incident management framework

Information Asset Owner

Information asset owners are senior/responsible individuals involved in running the relevant service. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

Information Asset Owners are responsible for risk assessing the organisational assets and reporting any risks to the SIRO.

Information Sharing

The seven golden rules of Information Sharing:

1. **Remember that the Data Protection Act** is not a barrier to **sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.
2. **Be open and honest with the person** (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 if you are in any doubt**, without disclosing the identity of the person where possible.
4. **Share with consent** where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being**: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, 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 people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.
7. **Keep a record of your decision and the reasons for it** – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

(Information Sharing: Guidance for practitioners and managers, p 11, 2008)

The Confidentiality Rules

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

(A guide to confidentiality in Health and Social Care, P 9, 2011)

Registration Authority and Smartcards

What is a Smartcard?

A Smartcard enables access to NHS systems and applications using access controls related to the access required to perform a job role. A Smartcard is like a debit or credit card – it is used with a passcode. It has a name, photo and unique user identity number printed on the Smartcard.

No information is stored on the Smartcard but it provides access to patient information if a legitimate reason to do so has been identified for a particular staff role. Any information accessed via the Smartcard needs to be kept secure and confidential, as with any personal or sensitive information. All staff are bound by their own professional codes of conduct, local regulations and policies, contractual requirements, the Data Protection Act and the NHS Code of Confidentiality.

Smartcards are also being used for other non-clinical access, such as remote access to the organisation's file structure. Although it is not being used to access clinical information, the security requirements of the Smartcard remain the same.

Smartcard Security

A Smartcard passcode is similar to a digital signature in that every time a Smartcard is used, the staff member is agreeing to comply with the terms and conditions of the national Registration Authority policy. Each time a Smartcard is used to log on, access is automatically monitored and alerts raised where access does not appear to be justified.

Passcodes should never be shared or written down. They should not be left unattended, on a desk. If a Smartcard is lost or damaged, the Sponsor or line manager should be informed as soon as possible.

Registration Process

The Registration Authority (RA) controls the issuing of Smartcards and manages the registration process. The RA team follows local and national processes, policies and procedures. To be issued with a Smartcard evidence of identity must be provided. Please see below for RA contacts.

For further information, please contact your local Registration Authority nhis.servicedesk@notts-his.nhs.uk

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a tool which can help organisations identify the most effective way to comply with their Data Protection obligations and meet individuals' expectations of privacy. The Information Commissioners Office (ICO) has developed a framework for organisations to use when considering a PIA and from that local guidance has been developed and amended specifically for health organisations.

An effective PIA will allow organisations to identify and fix problems at an early stage in a project - allowing them to be addressed before too much development and planning has been undertaken. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, a declaration of incompatibility with the Human Rights Act, or prohibitive costs in retro-fitting a system to ensure legal compliance or address community concerns about privacy.

A PIA should be carried out whenever there is a change that is likely to involve a new use or significant change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process, or information asset being introduced.

The procedure should be considered in any of the following circumstances:

- Introduction of a new paper or electronic information system to collect and hold personal data
- Update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information
- Design and development of a system where the personal data is held on a 'consent for holding and use' basis
- Changes to an existing system where additional personal data will be collected
- Proposal to outsource business processes involving storing and processing personal data
- Plans to transfer services from one provider to another that includes the transfer of information assets
- Any change to or introduction of new data sharing agreements.

This list is not exhaustive – if it is possible that there may be any impact on the use or processing of personal data, completing a PIA will enable the organisation to establish if there is a need to examine the processes in more detail. If assistance or guidance is required, please contact the Information Governance Team.

See the Contacts page for information on how to contact your local team.

Passwords

Choosing a password that is 'strong' will help to ensure that information is kept safe and secure. Please see the information below on creating a strong password.

- Ensure that a password is at least the minimum number required for the system being accessed: a minimum of 6 characters is usually required, however longer passwords are harder to break.
- Use English uppercase characters (A through to Z)
- Use English lowercase characters (a through to z)
- Use numbers (0 through to 9)
- Use special characters were possible (eg, % £ $ & # ! etc)

In addition,

- A password **must not** contain any part (eg, exceeding two consecutive characters) of a full user name.
- Do not choose a password that can be easily guessed (eg, relative's name, pet's name, favourite sports team).
- Always keep a password secret and never share a password with anyone, including any IT or other helpdesk. .
- Do not use the word 'password'.
- Try to use phrases to help make a base for a more complex password (eg, Mary had a little lamb = mhall).
- Change your passwords regularly.
- Do not type your password when others can see what you are typing.
- Never write your passwords down.
- Do not use the same password for all applications.

Even the most sophisticated computer system is only as strong as the users who access it and measures such as passwords help to prevent unauthorised access. If a weak or poorly concealed password is used there is the potential for unauthorised access through hacking. All activity on an account is deemed to have been made by the user and unauthorised access is a criminal offence.

Safe Haven Procedures

Safe Haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure that confidential person identifiable information (eg, patient and staff information) can be communicated safely and securely.

Safe Haven procedures act as a safeguard for confidential information which enters or leaves the organisation, whether this is by facsimile (fax), email, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the Safe Haven Procedure.

Staff are responsible for ensuring they handle person identifiable / sensitive / corporate sensitive data with care and respect. It is everyone's responsibility to protect this information from those who are not authorised to use or view it. All staff must ensure that whilst in their care, they have done everything possible to protect these types of information.

It is the responsibility of the sender of the information to ensure the information is received securely by the intended recipient.

Key Principles for Safe Haven working:

Safe Haven Emails:

1. Check that the recipients email address is correct.
2. Check that it is one of the secure domains (see NHSmail section)
3. Check that the information is being sent from a secure domain, eg NHSmail.
4. Send a test email to the recipient asking for acknowledgement of receipt of the email prior to sending the confidential information.
5. Ask the receiver to acknowledge receipt of the confidential information.

Please see the Safe Haven Procedure for additional information on post, phone and fax procedures. Please note that faxes are to be discouraged unless they are the only method available. In this case, ensure that all fax safe haven procedures are complied with.

For further information the Safe Haven porocedure and additional guidance are available on the publication scheme:

- M&A
- N&S

NHSmail (nhs.net)

NHSmail is a secure email service specifically designed to meet the needs of the NHS. It is available to all staff working within the NHS in England and Scotland and is also

available via NHS sponsorship to NHS business partners working with the NHS that require secure email systems. Plans are currently in place to upgrade the service to NHSmail2 which will enable secure email messages between NHS and non NHS organisations, including secure email between the NHS and patients, and is scheduled to be available at the end of 2015.

NHSmail is the recommended secure method for exchanging personal confidential data between NHS organisations and may be used for transmission of data between any government secure domain. The government secure domains are:

- NHS (*.nhs.net)
- GSi (*.gsi.gov.uk)
- CJX (*.pnn.police.uk)
- GSE (*.gse.gov.uk)
- GSX (*.gsx.gov.uk)
- GCSX (*.gcsx.gov.uk)
- SCN (*.scn.gov.uk)
- CJSM (*.cjsm.net)
- MoD (*.mod.uk)

NHSmail accounts end in 'nhs.net' and are separate from CCG provided emails which end in 'nhs.uk'. **Email accounts which end in 'nhs.uk' should not be considered secure for sending personal or sensitive information.**

It is important to ensure that any person identifiable or sensitive information is only exchanged between email addresses from secure domains (as noted above) so that the information contained in the message remains secure. Failure to do so could result in an incident being generated.

NHSmail is available from any internet-connected computer and also provides an online calendar and a global address book.

For further information regarding NHSmail click here:
http://systems.hscic.gov.uk/nhsmail

If you have difficulties setting up an NHSmail account, contact ext. 4040 or nhis.servicedesk@notts-his.nhs.uk .

Physical Security

ID Badges

All employees must ensure that they securely keep their ID badges and security card on their person at all times whilst onsite and that the ID and security card is not shared with any other person.

When visiting other sites in the course of your work, ensure that ID and security cards are visible or available if requested. When not at work, ensure that ID and security cards are kept securely.

All employees must return their ID card and or security card to their Line Manager upon the conclusion or termination of employment with the organisation.

Lost, Stolen, Damaged or Faulty ID cards

In the event that an ID or security card is lost, stolen, damaged or faulty it should be reported to a Line Manager in the first instance. The Line Manager will need to complete the appropriate form for their site and an incident form will need to be completed.

Laptop Security

Organisation laptops provide a portable and convenient mobile working solution and provide business benefits for the user. Laptop users must be vigilant at all times regarding the type of information/data being accessed to ensure that sensitive information/data is not seen by fellow commuters or other people in the area. Laptops are also an attractive target for thieves and extra precautions must be taken to ensure the safety of the device.

Users should follow the guidance below to minimise the risk of theft, loss or inappropriate access or viewing of data:

- Users should take all possible measures to avoid the laptop being stolen.
- Laptops should never be left unattended in a public place.
- When at home, laptops should be stored securely and only used by the authorised user.
- Laptops should be carried in an appropriate case or bag when away from organisation premises.
- Laptops should never be left in sight, for example on the seat of a car.
- Care should be taken when using laptops in public places to prevent casual observation of the screen. Unless absolutely necessary, sensitive information should never be worked on in public places.

For further information on mobile working, the CCG policies are available on the publication scheme:

- M&A
- N&S

Removable Media

Removable media can be classified as any portable device that can store and/or move data.

These include, but are not limited to:

- Optical disks (eg CD or DVD ROM)
- External hard drives and zip drives
- Magnetic tapes
- Solid state memory devices including USB memory sticks, pen drives, memory cards
- MP3 players
- Mobile phones
- Digital cameras
- Personal digital assistants (PDAs), (eg Palm, Blackberry)

Other mobile devices include laptops, tablet PCs, iPads.

Only devices which have the NHS approved standard of encryption, which is currently 256 bit AES, may be used to encrypt and protect NHS data. Unencrypted devices must not be used to transport or store personal or sensitive or NHS data.

Staff and contractors are not permitted to use any removable media other than those provided or explicitly approved for use by the organisation.

Should you require any further advice or guidance regarding removable media, please contact your local IT service desk or the Information Governance Team. See the Contacts page for information on how to contact your local team.

Security Awareness

Report suspicious activity

Always report any suspicious email or other electronic activity to the IT Service Desk. Part of their job is to stop cyber-attacks and to make sure the organisation's data is not lost or stolen.

Suspicious emails and links

Do not open suspicious links or attachments in emails. Opening an email will not infect your computer with a virus, but clicking on a suspicious link or email attachment may do. Opening suspicious links can compromise your computer and create unwanted problems without your knowledge.

Always delete suspicious emails and links.

Do not install unauthorised programs on your work computer

If you like an application and think it will be useful, contact the IT Service Desk and ask them to look into it for you. Do not download software from the internet.

For further information on IT queries contact your local IT Service Desk ext. 4040
or nhis.servicedesk@notts-his.nhs.uk

Clear Desk & Clear Screen

Information Governance and Information Security encourage methods which significantly reduce the risks associated with security breaches and incidents occurring.

It is essential that organisations implement high standards of handling information, data, and records containing patient or person identifiable data securely. Maintaining the confidentiality of all individuals for whom information is held and processing information by adhering to best practice governance guidelines and the law is essential.

Listed below are some actions that can be done to minimise the likelihood of a data breach or security incident occurring:

- Lock away all patient or personal confidential data (PCD), including sensitive and valuable documents (paper and removable media) in cabinets or desk drawers, as appropriate.
- Lock workstations (computers, laptops, terminals) when away from the desk, even for a short time, but pressing simultaneously **Ctrl + Alt + Delete** and selecting **Lock Work Station**.
- At the end of the day, close down all applications and log off or shut down the work station, as appropriate.
- Laptops must be stored securely and not left out on the desk when the user is not in attendance in the office.
- Ensure any documents or removable media such as CDs, DVDs, memory sticks etc are safely stored when not required at work, or at home should records or information need to be taken home.
- It is the responsibility of each user to ensure the security and the confidentiality of the information they have access to and to protect that information accordingly.
- When required to access and process sensitive information, be mindful of who can see the screen and position the screen where sensitive information cannot be viewed by anyone who is unauthorised to do so.
- If it is necessary to leave the office quickly in an emergency, for example a fire alarm, ensure the work station is locked if it is safe to do so, in order to prevent unauthorised access.

Incident Reporting

Reporting an Incident or Near Miss

All incidents and near misses must be reported to the line manager as soon as possible after the event. An incident or near miss could include letters or emails sent to the wrong individual or received in the incorrect department.

All incidents, near misses and serious untoward incidents must also be recorded on the organisations local Incident Report Form and forwarded to the line manager and to the appropriate Corporate Governance Manager at the CCG.

Whenever possible the incident Report form should be completed and submitted within 24 hours of the incident occurring.

The person involved in or identifying the incident in conjunction with a senior person on duty should complete the incident report.

In circumstances where a member of staff is unable to complete the form due to illness or injury, the senior person on duty should complete the incident report form.

Where an incident results in an absence from work of more than seven consecutive days (excluding the day of the incident, but including week-ends, bank holidays or days off) then the Line Manager must notify the Corporate Governance Manager in order that the Health and Safety Executive can be informed within fifteen days of the accident or incident occurring. This is a legal requirement under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulation (RIDDOR).

The CCG policies are available on the publication scheme:

- **M&A**
- **N&S**

Useful Information and Contacts

Should you require further advice or guidance with reference to Information Governance or Information Security please contact the GEM CSU Information Governance Team.

Useful Links

Information Governance Training via the Health and Social Care Information Centre IG Training Tool: https://www.igtt.hscic.gov.uk/igte/index.cfm

Records Management: NHS Code of Practice:
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

Confidentiality: NHS Code of Practice:
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Guide to Confidentiality in Health and Social Care:
http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

Caldicott 2 Report: Information: To Share or Not to Share – The Information Governance Review:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Information Commissioners Office:
http://www.ico.gov.uk/

Information Sharing: Guidance for practitioners and managers:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

Information Sharing: Guidance for practitioners and managers:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

Glossary - Information Governance Terms & Abbreviations

Abbreviation	Meaning
ADT	Admissions Discharges and Transfers
AES	Advanced Encryption Standard
AHP	Allied Health Professional
AHR	Access To Health Record request
AQP	Any Qualified Provider
ASH	Accredited Safe Haven
AUP	Acceptable Use Policy
BAU	Business As Usual
BC	Business Continuity
CAB/C&B	Choose and Book
CAG	Confidentiality Advisory Group
CCG	Clinical Commissioning Group
CDS	Commissioning Data Set
CEfF	Controlled Environment for Finance
CEO	Chief Executive Officer
CfH	Connecting for Health (now replaced by NHSE and HSCIC)
CG	Caldicott Guardian
CO	Chief Officer
CSU	Commissioning Support Unit
CTP	Commercial Third Party
DFM	Data Flow Mapping
DH/DoH	Department of Health
DMIC	Data Management Information Centre (Now known as DSCRO)
DPA	Data Protection Act
DR	Disaster Recovery
DSA	Data Sharing Agreement
DSC	Data Sharing Contract
DSCN	Data Set Change Notice
DSCRO	Data Service for Commissioners Regional Office (previously DMIC)
EDMS	Electronic Data Management System
eDSM	Enhanced Data Sharing Model (TPP SystmOne)
EPR	Electronic Patient Record
EPS	Electronic Prescribing Services
ESR	Electronic Staff Record
FOI(A)	Freedom of Information (Act)
GEMCSU	Greater East Midlands Commissioning Support Unit
GP	General Practice
GPES	General Practice Extraction Service
HES	Hospital Episode Statistics
HIS	Health Information Service/System
HPA	Health Protection Authority
HSCIC	Health & Social Care Information Centre
IAA	Information Asset Administrator

IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IGC	Information Governance Committee
IGM	Information Governance Manager
IGSoC	Information Governance Statement of Compliance
IGT	Information Governance Toolkit
IGTT	Information Governance Training Tool
IM&T	Information Management and Technology
ISA	Information Sharing Agreement
ISP	Information Sharing Protocol
KPI	Key Performance Indicator
LAs	Local Authorities
LES	Local Enhanced Service
LSP	Local Service Provider
NACS (Now ODS)	National Administrative Codes Service
NHAIS	National Health Applications and Infrastructure Services
NHSCB	NHS Commissioning Board (previously NHSE)
NHSE	NHS England
NWW	NHS Wide Web
ODS (Previously NACS)	Organisation Data Service
PCD	Personal Confidential Data
PCT	Primary Care Trust
PHE	Public Health England
PIA	Privacy Impact Assessment
PID	Personal Identifiable Data (previously PCD)
QIPP	Quality Innovation Productivity and Prevention
QOF	Quality Outcome Framework
RA	Registration Authority
RISC	A risk stratification tool supplied by Health United UK
SAR	Subject Access Request
SBS	Shared Business Service
SI/SUI	Serious Incident/Serious Untoward Incident
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
SME	Subject Matter Expert
STEIS	Strategic Executive Information System
SUS	Secondary Uses Service
VSO	Voluntary Services Organisation

Definitions

Anonymisation – a process where all information that could identify an individual is removed. The information can then be used for secondary purposes i.e. non health care without needing the consent of the patient.

Primary Use of data – is when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

Pseudonymisation – reversible anonymisation i.e. the identity of an individual can be found if access to the correct software, encryption key etc is possible.

Weak pseudonym (such as NHS number or postcode) - The classification of a weak pseudonym stems from the fact that unless a user has access to another system that requires authorisation and user authentication etc (eg Exeter or the Spine) then the individual cannot be identified from the NHS number alone.

In November 2013 the Confidentiality Advisory Group (CAG) stated that the term 'weakly pseudonymised' should no longer be used and that the precise identifiers (eg NHS number or post code) should be stated, although you may still see the term referred to in documents.