NHS
Hull
Clinical Commissioning Group

NHS
East Riding of Yorkshire
Clinical Commissioning Group

Information Governance and Data Security

User Handbook

Version 13

CONTENTS

1.0 INTRODUCTION TO INFORMATION GOVERNANCE

"Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information"

Health and Social Care – What you should know about Information Governance Booklet Pg 2

Information Governance includes the following:

- Data Protection/Confidentiality
- Caldicott
- Information and cyber security
- Records Management and Data Quality

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information plays a key part in clinical governance, service planning and performance management and therefore it is essential that all health organisations ensure information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically, and
- Shared appropriately and lawfully
- Arrangements for secure disposal

1.1 How This Guidance Will Help You!

This guidance provides staff with a brief introduction to Information Governance and summarises the key user procedures that have been developed to support Information Governance in the organisation. The aim of this booklet is to ensure that you are aware of your roles and responsibilities for Information Governance.

Everyone is responsible for Information Governance

2.0 KEY INFORMATION GOVERNANCE ROLES

A number of key Information Governance related roles exist, which you need to be aware of.

Senior Information Risk Owner (SIRO)

The SIRO is responsible for, and takes ownership of, the organisations risk policy and all aspects of risk associated with information governance, including those relating to confidentiality and data protection. The SIRO is the Board level lead for information risk.

Caldicott Guardian

The Caldicott Guardian is responsible for, and takes ownership of, ensuring that the organisation satisfies the highest practical standards for handling patient identifiable information. Any sharing of identifiable data should be reviewed by the Caldicott Guardian first.

Data Protection Officer (DPO)

The Data Protection Officer offers expert knowledge of data protection law and practices.
These are:

- to inform and advise the organisation and its employees about their obligations to comply with the General Data Protection Regulation (GDPR) and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including assigning responsibilities, managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to cooperate with the Information Commissioner's Office (ICO)
- to act as the contact point for the ICO and for individuals whose data is processed (employees, patients etc.).

Under GDPR, the role of DPO is protected and the organisation must ensure that:

- The DPO reports to the highest management level of the organisation – i.e. Governing Body level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Information Governance Lead

The IG lead is responsible for ensuring effective management, accountability, compliance and assurance for all aspects of information governance within the organisation.

Information Asset Owners (IAOs)

The Information Asset Owner is a senior manager who takes responsibility for the security of information of a specific information system or systems within the organisation, as well as understanding and taking ownership of the risks relating to the organisational assets and to provide assurance to the SIRO.

Information Asset Administrators (IAAs)

The Information Asset Administrator is responsible for the day to day running of one or more information systems and for ensuring that policies and procedure are adhered to, bringing any actual and/or potential risks to the attention of the IAOs.

3.0 INFORMATION GOVERNANCE POLICY

The purpose of the Information Governance policy is to set out the organisations IG Framework in order that appropriate processes and controls are put in place to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental.

The Information Governance Policy details:

- The regulatory and legislative requirements
- How information is protected against unauthorised access
- Appropriate policies and procedures are put in place to instruct staff in their responsibilities
- How confidentiality of personal confidential information is assured
- How integrity of the information and good data quality practices are maintained
- Information is available to authorised personal when they need it in order to do their job
- Data Security and Data Security Awareness training requirements
- The role of Business Continuity and Disaster Recovery plans
- That all breaches of information security, actual or suspected, must be reported to, and investigated by the Data Protection Officer

The policies and procedures that were produced to support the policy apply to this organisation and all its employees, executive and non-executive staff, agency staff, seconded staff and contractors. The policies and procedures will be reviewed annually in accordance with the requirements of the Information Governance toolkit or upon significant internal/external changes and in conjunction with annual security audits. All staff will be informed of updates.

Additional supporting policies and procedures will cover these areas:

- Information Security
- Training
- Induction and Recruitment
- Network Security
- Registration Authority – this is the issue and management of smartcards
- Data Handling - Best Practice
- Exchanges of Information
- Email and Internet
- Incident Management
- Business Continuity/Disaster Recovery
- Confidentiality and Data Protection
- Safe Haven /Secure Transfer
- Information Sharing

It is the responsibility of each employee to adhere to the policy and underpinning procedures, to know where Information Governance policies can be accessed and to have read and understood them.

4.0 PERSONAL CONFIDENTIAL DATA

Personal Data

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

- Name
- Date of birth
- Post code
- Address
- Online identities (usernames, IP addresses) and/or location (GPS) data
- Photographs, digital images etc.
- NHS number
- Date of death
- Pseudonymised data

Special Categories of Personal Data

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

- Physical and mental health
- Genetic data
- Biometric data
- Social care
- Ethnicity and race
- Sexuality
- Trade union membership
- Political affiliations
- Religion

Records relating to criminal charges and offences are also be treated as a special personal data.

The organisation places great emphasis on the need for the strictest confidentiality in respect of personal confidential data and especially on sensitive personal data. This applies to manual and computer records and conversations about patients' treatments. Everyone working for the organisation is under a contractual and legal duty to keep personal information, held in whatever form, confidential. The patients and individuals who feel their confidentiality has been breached may raise a complaint under the complaints or grievance (for staff) procedure.

All organisations carrying out functions as part of, or on behalf of, the NHS have a contractual requirement to maintain the confidence to those whose information they process, e.g. patients, staff etc.

Your responsibilities to comply with the Common Law Duty of Confidentiality

All employees working in or on behalf of the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidentiality, the Data Protection Act and the General Data Protection Regulation. It is also a requirement within the NHS Care Record Guarantee and NHS Constitution, produced to assure patients regarding the use of their information.

A duty of confidence when handling privileged information is upheld by common law, statute, contract of employment, disciplinary codes and policies and professional registration. Additionally, some non-personal information may be considered sensitive, such as those relating to contract tenders.

Where personal confidential or otherwise sensitive data is held then the organisation needs to take appropriate measures to ensure that it is secure and confidential.

If there is no ongoing need to retain data in an identifiable form, then it should be pseudonymised/ anonymised as soon as possible to reduce risk of inappropriate retention, disclosure or loss.

5.0 ACCESS TO PERSONAL INFORMATION

5.1 Staff access to personal confidential information

All staff should be aware that all access made to electronic records is recorded and auditable that audits are run periodically on all systems to check that access made to records is legitimate and required as part of a patient's healthcare pathway.

All staff are personally liable for breaches of the Data Protection Act and General Data Protection Regulation (GDPR) and may be subject to the organisations' disciplinary procedures, fined and/or and can be prosecuted in addition to the organisation itself being fined by the Information Commissioners Office.

5.2 Individuals requesting access to personal confidential information

Individuals (such as patients or staff members) have the right to request access to personal information held about them by the organisation, under the Data Protection Act and GDPR, this was previously known as a Subject Access Request (SAR). The organisation will have a SAR process in place which all staff will need to be familiar with so that they know who to pass a request on to should they receive one.

Healthcare organisations should endeavour to meet such requests within a 21 day timescale and where this is not possible they must be either completed within a statutory one month period or an explanation provided as to why a further month is required.

6.0 SHARING AND USE OF PERSONAL INFORMATION

Information that can identify individual patients must not be used or disclosed for any other purpose than direct healthcare other than where:

- The individual patient or patients have given their explicit consent for the information to be used for specific purposes
- There is a legal obligation to disclose the information (e.g. Court Order)
- There is an overriding public interest to disclose the information; you will need to consult with your DPO to confirm this

Where any personal information is used or considered for use by the organisation, there must always be legal basis for that use. Where you share personal information with other organisations, conditions must be adhered to as set out in the relevant Information Sharing Protocol.

Where there is a need to process and share identifiable information only NHS Number should be used as the identifier. Where there is a clear legal basis, NHS Number should be used across health and social care organisations.

There is a reinforced duty for health and social care professionals to share patient information as part of the direct care of that individual. This does not however apply to any secondary or other uses of identifiable patient data, which can only be shared with a clear legal basis being in place and clearly identified to the individuals concerned.

NATIONAL DATA OPT-OUT

The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning. Before you disclose any personal information you must ensure that you have taken into account whether the national data opt-out is applicable. It is not applicable for direct care or for the use of anonymised data. More information can be found at the link below or from your IG lead.
https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out

7.0 INFORMATION GOVERNANCE USER PROCEDURES

7.1 Information Security – Staff Responsibilities

DO…

- Remember that you have signed a confidentiality agreement within your contract of employment
- Be aware of information governance policies and procedures
- Be aware of your responsibilities for information security
- Be aware that unauthorised access to disclosure of or misuse of personal data will be treated as a serious disciplinary offence and will be required to be reported to the Information Commissioner with the possibility of personal fines and/or prosecution
- Ensure that temporary staff and third party contractors complete mandatory Data Security Awareness training and also sign a confidentiality agreement as part of the induction process (available from the Information Governance Lead)
- Remember that you are responsible for ensuring that you are up to date with all Mandatory training to enable you to carry out your work efficiently and securely. This is both a contractual and legal requirement and may lead to disciplinary action for you and substantial fines by the Information Commissioner on the Organisation
- Ensure your training needs are assessed on a regular basis
- Report potential concerns or security weaknesses to your line manager
- Know how to report security incidents (see how to report an information security incident in section 7.12)
- Be aware that the organisation has a formal disciplinary process for dealing with staff that violate the organisations' policies and procedures

DO NOT…

- Attempt to prove a suspected security weakness, as testing a weakness might be interpreted as a potential misuse of the system
- Allow third parties access to the organisations, hardware and equipment, without correct authorisation
- Be afraid to challenge anyone who you were not aware would be in the organisation
- Ignore security incidents

7.2 Physical security

DO…

- Report the loss of your access keys or card immediately to your line manager
- Ensure all IT equipment is reasonably protected against theft and unauthorised access
- Follow the procedures for use of laptops, portable devices, mobile phones and removable media and ensure that if you use a blackberry, that it is password protected- see section 7.3 Use of Portable Devices
- Ensure that assets are disposed of in accordance with organisational policy
- Wear an ID badge
- Issue visitor badges so staff can identify visitors who may not be familiar with organisational policies and restrictions
- Challenge unidentified visitors in controlled areas
- Escort visitors in secure areas at all times
- Operate a clear desk and clear screen policy
- Ensure confidential and patient information is locked away when not required
- Ensure that confidential waste is stored securely prior to disposal and certificates of destruction are obtained
- Ensure incoming and outgoing mail points are in secure areas
- Clear confidential and personal confidential information away from printers and fax machines immediately
- Ensure PC's are not left logged on and unattended- Ctrl-Alt-Delete, then click lock computer
- Ensure keys to premises are securely stored
- Ensure that secure areas are kept secure and locked when not in use
- Site computer screens away from unauthorised viewing
- Ensure that all deliveries are correctly checked, recorded and distributed in a secure manner

DO NOT…

- Take equipment, information or data off-site without prior authorisation
- Leave equipment, information or data unsecured in public areas
- Tell others what keys or access codes you have been entrusted with

7.3 Environmental security

DO…

- Be aware of the building fire procedures
- Know who the fire officer is
- Attend a fire lecture on an annual basis or complete the mandatory e-learning module
- Keep fire doors closed
- Know where the fire extinguishers are
- Ensure that fire exits and manual fire alarms are accessible
- Maintain a neat and tidy environment to help limit the spread of fire
- Ensure that any heat source is always properly operated and maintained in accordance with fire regulations; this especially applies to electric cables
- Ensure that cabling does not trail and the electric source is not overloaded
- Be vigilant for the risk of water damage

DO NOT…

- Store flammables near to any source of heat
- Site equipment near to sources of water e.g. radiators, water pipes, water tanks, air conditioning, pot plants, vase of flowers etc.
- Attempt to tackle an outbreak of fire unless you are almost certain that it can be easily extinguished by the appropriate hand held extinguisher.

7.4 User Access Control and password management

DO…

Ensure that a user ID and password is required for access to the network and any applications containing personal information.

Select quality passwords with a minimum of eight characters which are:

- Relatively easy to remember
- Not based on anything somebody else could easily guess e.g. names, telephone numbers, date of birth etc.
- A combination of upper and lower case letters, numbers and symbols
- Not use old or re-cycled passwords
- Keep passwords confidential – YOU are responsible for information entered using your password. Failure to protect YOUR password or workstation could result in disciplinary action
- Change passwords at regular intervals (and also if there is any indication of a possible system or password compromise)
- Lock your computer when away from your desk (activated by ⊞+L or Ctrl+Alt+Del, lock computer)
- Be aware that you are responsible for any activity performed under your logon ID and password. This includes any activity undertaken by someone else whilst your PC is left logged in and unattended without a password protected screensaver
- Ensure that you log off correctly (i.e. don't just switch the machine off)
- Contact the IT Service Desk if you have forgotten your password and need your access to be reset
- If you are a line manager- terminate a staff member's network access or Smartcard rights when they leave your organisation

DO NOT…

- Leave a PC logged in and unattended (press ⊞+ L or Ctrl-Alt-Del, then click lock computer) to secure your PC
- Use someone else's ID or login or allow anyone to use yours (this is a serious disciplinary offence and all access is auditable)
- Write a password down (unless you can store it securely)
- Connect any unauthorised hardware or download software to the organisation network

7.5 Use of portable IT devices

Portable devices include mobile devices, cameras and mobile phones.

Removable data storage media include any physical item that can be used to store and/or move information. This could be a USB stick, CD, DVD, memory cards or digital storage devices.

Unencrypted personal data held on portable devices present a huge risk to the organisation if lost or stolen.

YOU MUST ENSURE THAT:

- Only authorised staff have access to portable computer devices and digital storage devices such as USB's etc. All portable equipment that contains personal and confidential information must be encrypted. There are no exemptions to this rule and you will be held personally responsible if you download such data to an unencrypted device. If you are unsure whether your device is encrypted please contact the service helpdesk
- A register is maintained where portable equipment is used in a pool to enable the identification of the current user
- Any backups taken from portable devices should always be encrypted to NHS Standards and stored securely
- Any loss or theft of portable equipment is reported immediately to the police and your line manager
- If you have been issued with an encrypted laptop for use in your organisation, you must log the laptop onto the network at least once every three months to ensure that the encryption password remains valid
- Use portable media for short term storage only - ensure it is backed up to the server frequently

DO NOT…

Store identifiable information on removable media unless it is absolutely necessary and if so, ensure it is password protected and encrypted

- Leave portable equipment in places vulnerable to theft
- Leave equipment unattended in public areas
- Leave portable equipment visible in a car, always lock it away in the boot during transit but never store it in an unsupervised car (due to risk of vehicle theft)
- Delay in reporting any lost or stolen equipment to the police and your manager
- Connect any unauthorised equipment to the network mp3 players, cameras, wireless routers- if in doubt, contact the IT service desk
- Install unauthorised software or download software from the internet without authorisation from IT
- Allow unauthorised personnel to use the equipment, e.g. household members

7.6 Terms and conditions of use of smartcards

Individual smartcards are issued to organisation team members who require access to specific clinical systems. Smartcards provide you with the appropriate level of access to healthcare information that you need to do your job.

Remember – You have a duty to keep patient information secure and confidential at all times and the terms and conditions of use mean that you:

DO…

- Read and follow the declarations and terms and conditions for smartcard users
- Understand that NHS smartcards help control who accesses what and at what level
- Using the same technology as chip and pin, members of staff are identified by names, by photograph and a unique identity number

DO NOT…

- Share individual smartcards
- Allow anyone to use your smartcard—checks on access will be made and you will be held responsible for all patient data accessed and or recorded using your smartcard
- Leave your smartcard unattended at any time
- Access any record / information you do not have a legitimate right to access

7.7 Protection against malicious software

DO…

On discovering a virus:

- Note any symptoms and immediately disconnect the computer from the network
- Contact the IT service desk immediately

DO NOT…

- Attempt to clear an infected PC yourself
- Accept any freeware as it may contain spyware or a virus
- Review to ensure all relevant items detailed e.g. emails

7.8 Software, data and media management

DO…

- Respect all computer software copyrights and adhere to the terms and conditions of any licence to which the organisation is a party
- Actively and frequently undertake housekeeping of your data, e.g. delete unwanted files regularly as information is soon out of date
- Archive files and documents on a regular basis in line with your retention policy or in line with the IGA Records Management Code of Practice
- Ensure that tapes and disks are disposed of securely, contact IT Services for support

7.9 Data handling

DO…

- Lock any manual patient records, such as Lloyd George envelopes away when not in use
- Ensure that confidential conversations are held where they cannot be overheard by members of the public or other staff and ensure that sensitive medical issues are only discussed in private consultation areas
- Encrypt any confidential/sensitive information which needs to be emailed from the organisation unless sending nhs.net to nhs.net. In the case of sending of extremely sensitive information consider sending a test email first
- Ensure that all waste containing patient or staff identifiable information is cross shredded before disposal using shredding consoles
- Ensure that envelopes containing personal confidential data are clearly and correctly addressed, marked 'confidential' and the senders address included
- Be aware of safe transfer guidelines for confidential information e.g. noting that faxes should only been sent in emergency situations.
    - Contact the recipient to let them know that the fax is being sent
    - Check the number dialled and check again before sending
    - Where possible use pre-stored numbers
    - Ask the recipient to acknowledge receipt
- Ensure that envelopes containing personal confidential data sent via internal or external mail are clearly and correctly addressed, marked 'confidential' and the senders address included
- Always take care when making a phone call to ensure you are not going to be overheard when discussing individuals

DO NOT…

- Leave information where it can be viewed by someone who does not have a legitimate right to view it
- Discuss patient or staff details where you may be overheard
- Disclose or share information to someone where there is not a legal basis to do so
- Leave confidential messages on answering machines or text patients without their prior consent

7.10 Email use

DO…

- Be aware that the email system is primarily for business use. Occasional and reasonable personal use may be permitted provided that it does not interfere with the performance of your duties and does not conflict with organisational policies. You must not use any work provided resources, such as email, for any private commercial or financial activity.
- Personal emails should include "Private" in the subject.
- Be aware that your mailbox and its contents (including personal email) may be accessed by others without notice. Follow the email policy for email etiquette acceptable use and the retention of messages
- Be aware that the same laws apply to email as to any other written document
- Use a signature which must include your contact details e.g. name, telephone number and work address
- Be careful about what you type, particularly referring to individuals - email is easily forwarded
- Use an out of office message to advise people when you are not available and who they can contact during the absence
- Ensure email delegates are set up appropriately, to allow access to your emails whilst out of the office, on holiday etc.
- Use the address book (or contacts) where possible and consider turning off autocomplete, to prevent incorrect addressing
- Report to your Line Manager and IT Service Desk any email that you receive or become aware of, that may be regarded as illegal or offensive
- Be aware that your mailbox may be accessed if you are absent, e.g. sickness or holiday
- Remove any personal contents from your mailbox and personal network folders when leaving employment; (it may be made available to a replacement or line manager)
- Personal, sensitive or confidential information must be sent by secure email, e.g.NHS.net to NHS.net or by inserting [secure] at the start of the email subject

DO NOT…

- Send sensitive or confidential information via an insecure email address unless it is encrypted by using [secure] in the subject
- Attach large files to emails (+10mb) - where possible send a link to the file or send as a zip file it to reduce its size
- Send email that is or which could be considered to be sexually or racially offensive, pornographic, defamatory, abusive, criminal or for any other unauthorised purpose
- Create or forward chain email
- Send emails to large numbers of people unless it is directly relevant to their job
- If sending to a group of patients or the public, use bcc unless it is either necessary or the other recipients have agreed to share their addresses
- Set up an auto-forward of your work emails to a home email address i.e. hotmail, yahoo
- Do not use your email account for permanent storage of work related issues

7.11 Internet use

DO…

- Be aware that the use of the internet is primarily for business use unless otherwise agreed with your employer and that all use may be monitored and restricted
- Be aware that any inappropriate use of the internet may result in prosecution and/or disciplinary action being taken against you
- Be aware of the internet and social media policy e.g. obtain approval from your line manager for any online activities associated with the organisation, e.g. by displaying an your organisations email address or anything about the organisation on social networking sites

DO NOT…

- Leave your computer unlocked whilst unattended

7.12 Incident Management

Incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the system or information being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to unauthorised access to data all of which will have an adverse impact to patients and to the organisation e.g.

- embarrassment to the patient/patients/organisation
- threat to personal safety or privacy
- legal obligation or penalty
- loss of confidence in the organisation
- financial loss
- disruption of activities

All incidents or information indicating a suspected incident should be reported as soon as possible to your organisation's Information Governance Lead. Details of incidents must be reported via the organisations' risk incident reporting system. Ensure all systems are regularly updated and security measures are regularly reviewed.

DO NOT…

- Keep an incident to yourself - ensure it is reported not only so that working practices can be improved but because information governance and information security breach reporting is mandated by law and not reporting such breaches could result in substantial fines and prosecution to the organisation and/or yourself.

7.13 Information Breaches

Incidents that are classed as a breach require additional reporting processes to those referenced in 7.12.

An information governance breach would be where, for example, there is a loss of personal information or where particularly sensitive personal information has been sent to the wrong person or location.

Where staff become aware of a breach they should inform the organisations Information Governance Lead who will review it against the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation, liaising with the Caldicott Guardian and/or SIRO as necessary. Incident reports are reported to the Governing Body through its subcommittee structure.

8.0 COMPLIANCE REQUIREMENTS

DO…

Be aware that the organisation is obliged to abide by relevant UK and EU legislation and guidance - the key ones are listed below:

- General Data Protection Regulation (EU) 2016/679
- Data Protection Act 2018
- Access to Health Records Act 1990
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Computer Misuse Act 1990
- The Network and Information Systems Regulations 2018
- Copyright, Designs and Patents Act 1998
- Human Rights Act 1998
- The Caldicott Principles
- The Health and Social Care Act 2012 (Includes sections on access to confidential information)
- The NHS Care Record Guarantee
- The NHS Constitution

DO NOT…

- Breach legal requirements
- Be ignorant of the legal requirements that affect you, if unsure, please ask your information governance lead
- Copy software or documents illegally or breach copyright laws, ask the copyright holder for permission

8.1 General Data Protection Regulation (GDPR)

It is important to note that GDPR gives the Information Commissioner increased powers and authority and the penalty for breach of the regulations is now capped at a maximum of €20,000,000 or 4% of the turnover of an organisation. They can also impose administrative fine of half these amounts on an organisation that fail to comply with data protection laws.

The six principles of the GDPR are as follows:

- **Lawfulness, fairness and transparency**

  - ✓ You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
  - ✓ You must ensure that you do not do anything with the data in breach of any other laws.
  - ✓ You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
  - ✓ You must be clear, open and honest with people from the start about how you will use their personal data.

- **Purpose limitations**

  - ✓ You must be clear about what your purposes for processing are from the start.
  - ✓ You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
  - ✓ You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

- **Data minimisation**

  You must ensure the personal data you are processing is:

  - ✓ adequate – sufficient to properly fulfil your stated purpose;
  - ✓ relevant – has a rational link to that purpose; and
  - ✓ limited to what is necessary – you do not hold more than you need for that purpose.

- **Accuracy**

  - ✓ You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
  - ✓ You may need to keep the personal data updated, although this will depend on what you are using it for.
  - ✓ If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
  - ✓ You must carefully consider any challenges to the accuracy of personal data.

- **Storage limitations**

  - ✓ You must not keep personal data for longer than you need it.
  - ✓ You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
  - ✓ You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
  - ✓ You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
  - ✓ You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
  - ✓ You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

- **Integrity and confidentiality / Security**

  - ✓ You must ensure that you have appropriate security measures in place to protect the personal data you hold.

- **Accountability**

  - ✓ The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.
  - ✓ You must have appropriate measures and records in place to be able to demonstrate your compliance.

Key changes that may affect your working procedures between GDPR and the previous Data Protection Act include:

- information breaches must be reported via the DSP Toolkit (to the ICO) within 72 hours of becoming known. This applies to breaches that would likely result in a risk to the privacy rights and freedoms of individuals. If there's a high risk you need to notify the individuals too.
- organisations must employ the 'data protection by design and by default' approach to activities involving personal data.
- A Data Protection Impact Assessment (DPIA) is required by law for any new system or project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- privacy notices must transparently explain how personal data is used and the rights of the data subject. It is important ensure the Right to be Informed is supported.
- Right of Access requests (where an individual requests access or a hold of the personal data being held about them) must be completed within a month and provided free of charge (unless a request is repetitive). Please note the NHS has a separate target of 21 days to fulfil valid requests.

8.2 The Caldicott Principles

The Caldicott Reports have identified weaknesses in the way parts of the NHS handle confidential patient data. Several Caldicott principles were developed, which provide a framework for the management of access to personal information within the NHS:

Principle 1: Justify the purpose(s) (for 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

8.3 NHS Digital Confidentiality rules

'A guide to confidentiality in health and social care' set out to demystify the complexities between the law, professional obligation and a duty of care towards the individual, it consists of five rules:

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

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

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

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

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

8.4 Business Continuity

Ensuring that the organisation has a robust plan to mitigate disruptions to its business are paramount in providing a reliable service to its customers.

Business continuity planning enables the organisation to:

- Assess the risk of a security failure or disaster occurring
- Analyse the consequences to the running of the organisation if a security failure or disaster was to occur
- Plan measures to reduce the likelihood of a security failure or disaster occurring
- Identify critical resources without which the organisation could not function
- Plan measure to allow the organisation to continue to function if a security failure or disaster does occur

DO…

- Identify your critical (to the organisation) resources
- Take preventative measures to guard against the likelihood of an incident occurring or having a major incident
- Decide what takes priority for recovery
- Have emergency contacts handy and up to date
- Prepare contingency plans for the most likely emergency situations
- Practice your plans on a regular basis
- Make sure everyone knows what to do and when
- Keep plans up to date by informing a change of contact details etc.
- Seek help and guidance for preparing and evaluating your plans
- Record any incidents which resulted in you testing the plan i.e. loss of electricity/gas supply

DO NOT…

- Think it will never happen to me
- Think that it is someone else's problem
- Make plans that are too difficult to follow
- Create a plan, and forget about it. It must be kept up to date to be useful
- Keep plans where you can't get to them, ensure you have one copy on site and one copy off site
- Use unrealistic scenarios for testing the plan e.g. a meteor landing on the building

9.0 TOP TIPS FOR PROTECTING CONFIDENTIALITY

Remember, information governance is common sense. Don't take risks with information and always handle it as if it were your own. Don't put yourself or your organisation at unnecessary risk. Any harm caused to patients/clients may result in a claim against you and/or your organisation. The Information Commissioner can also fine organisations up to €20,000,000 if information is recklessly lost or disclosed without due regard to policies and procedures.

Think about all information as if it were your own would you expect your information to be left available for anyone to view?

- Lock your computer - before leaving your desk always lock your computer by pressing ⊞+L Control-Alt-Delete-Return (lock computer), whenever you leave your desk **Remember, any work done under your login is attributable to you - even if you did not do it!**
- Passwords - NEVER share your login or password or use anyone else's login or password
- Smartcards - NEVER leave your smartcard unattended; always remove it when leaving your computer. Remember any inappropriate access under your smartcard can only be attributable to you!
- Faxes - should only be used in emergencies. If faxing personal or patient identifiable information always use a safe haven fax machine or safe transfer procedures.
- Emails - only send encrypted personal identifiable or business sensitive data by email (using nhs.net to nhs.net or [secure] in the subject)
- Paper information - think about how you handle paper information, would you leave your information on view for anyone to see- ALWAYS secure any information you are handling
- Memory sticks (USB/Flash drives) - it is policy that only encrypted memory sticks/USB drives are permitted for business purposes. See the Information Security policy.
- Post - identifiable information sent from the organisation should always be marked "Private and Confidential" and sent securely. If sending comprehensive records or relating to several people in one envelope, ensure that the envelope is robust and use an approved courier service or a secure postal service, such as recorded/signed for or traceable/special delivery.

10.0 TRAINING

All staff, including those on temporary or honorary contracts, secondments, volunteers, pool staff and students, are required to complete annual Mandatory Data Security Awareness Level 1 training without exception. The training is split into four learning modules with an additional "Welcome module". Each module takes up to 15 minutes to complete and concludes with an assessment.

The modules can be taken in any order and the system will record the pass marks and issue a certificate on successful completion of the five modules. It is recommended that you retain a copy of the certificate for your own records.

It is required that a minimum of 95% of all employees achieve at least the 80% pass mark.

The topics covered in the four modules are:

1. Introduction to security awareness
2. Information and the law
3. Data security - protecting information
4. Breaches and incidents

Training should be accessed through the Electronic Staff Record: https://my.esr.nhs.uk/.

If you are experiencing any difficulties with accessing the training, please go to https://portal.e-lfh.org.uk/ and register and login.

Information about registration, access to the training and ongoing support is available from http://support.e-lfh.org.uk/e-lfh-support-home.
Specifically for logging in, please see;
http://support.e-lfh.org.uk/get-started/logging-in-out/

Please note any queries about the e-LfH website must be directed to e-LFH at the link above as the IG Team do not facilitate this e-learning.

Remember, it is your responsibility to ensure that your annual Mandatory Data Security Awareness training is kept up to date - lapsed training could prevent you from incrementing or result in your organisation failing to provide the necessary assurances about how it handles information and administrative fines!

Produced by the Information Governance Team

INFORMATION GOVERNANCE AND DATA SECURITY DECLARATION FORM

I confirm that I have received the Information Governance and Data Security User Handbook and understand that it is my responsibility to read and understand it and to raise any queries or concerns with my line manager or directly with the Information Governance team.

This booklet has been developed to ensure that users are compliant with, but not limited to the General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patent Act 1988, ISO27001 and the Caldicott principles.

It is important to remember that **you** are accountable for your computer login and that all activity is auditable. Your email and internet activity may also be monitored. It is **your** responsibility to ensure that only you know your password and that if you leave your computer/device logged in and unattended you must lock your computer/device to stop any unauthorised use.

If you choose to make a note of any login/IDs and/or passwords that you are using, lock them away in a secure place. Keep all passwords and smartcards secure and **do not** share them with anyone.

You should be aware that inappropriate use, including any violation of organisational policies may result in the withdrawal of access and may result in prosecution and/or disciplinary action, including dismissal, in accordance with the organisation's disciplinary procedures.

Signed:	
Name (Please PRINT):	
Date:	
Job Title:	
Team:	
Email:	

Please note that once signed this declaration will be held on your HR record