Information Governance - Best Practice Guidelines

What is Information Governance?

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Common Law of Confidentiality
- Records management
- Information security

It covers every record you create, review, update and dispose of.

The following guidelines will help you to comply with your information governance responsibilities at work. Compliance with information governance is a requirement of your contract. If you are in any doubt about what actions you should take then please contact the Corporate Governance Officer Serena.Ellis2@nhs.net

Training

All CCG employees are required to complete information governance training through ESR.

1. New employees need to complete the training

2. If your role requires additional training the Information Governance Lead will inform you and/or it will be identified through the PDR process

Work Stations

1. Lock drawers/cupboards/filing cabinets before you leave, taking the key out of the lock

2. Wear you identify badge, and ask to see other people's identity badges if asking for personal information

3. Never leave personal information or confidential information on desks

4. Always lock away personal information and confidential information

Computers

1. Do not let other people see what's on your screen especially if

you work in busy areas where numbers of the public/patients have access.

2. Always keep your password confidential and never share it with anybody or write it down, especially near your work station.

3. Always use a strong password which includes both uppercase and lowercase letters, numbers and symbols i.e. P@5$w*0Rd

4. Log off or lock the screen (by pressing ctrl, alt, and delete at the same time when you're away from your desk.

5. Only use NHS approved pre-encrypted portable media

6. Never save documents to the C drive

Telephones

1. Do not to discuss personal information where you could be overheard

2. Always adhere to the following procedures if someone telephones asking for personal information:

    - Take their details and ring the person back, preferably via their switchboard
    - Ask for information requests to be sent in writing
    - Always try to check that the person you are speaking to is who they say there are. This is very important when dealing with patients and patient enquires
    - Be mindful of information sharing conditions or consent requirements to share personal information with others

Emails

1. Do not email any personal information outside of the local health economy unless it has been password protected.

2. When forwarding an email check that the whole of the email content is relevant and appropriate. Do not forward personal or confidential details unless necessary

3. You can send personal information from an 'nhs.net' account to another 'nhs.net' account. (Please refer to the Information Management and Technology Policy for any variances to this)

4. If in doubt then send a test email first and obtain confirmation of receipt

5. If sending an email which does contain personal information always adhere to the following:

    - Check the email address is correct
    - Check if you need to password protect information
    - Put all the personal confidential information into a document and attach to the email
    - Do not put personal information in the subject box
    - Check email has been received
    - In your email please always include your name, job title and contact details

Sending Faxes

You must only fax personal information to a safe haven fax, following the safe haven procedure of:

1. Checking if the information really needs to be faxed

2. Check the fax number of the person receiving the fax

3. Check recipient fax is a safe have fax

4. Telephone the recipient before you send the fax

5. Ask for confirmation that the fax has been received

6. Use safe haven fax front cover sheet

Records Management

1. Information should be destroyed in accordance with the Information Governance Alliance Health Records Management Code of Practice Retention Schedule: http://systems.digital.nhs.uk/infogov/iga/resources/rmcop/index_html

2. Corporate Records must be completed, maintained and filed in accordance with the Non Clinical Records Strategy

3. Never leave personal or confidential information lying on desktops

4. Under no circumstances should you access records of patients that you are not providing care for – including records of relatives, friends etc

5. If someone wants to access their health records or the records of a relative please direct them to the Information Governance Lead

Printing and Photocopying

1. All staff should now have a printer code which is required when printing any confidential and personal information

2. Check printers have paper and do not need replacement ink cartridges

3. Only copy confidential and personal information if absolutely necessary and do not keep longer than required (refer to the Information Governance Alliance Records Management Code of Practice Retention Schedule) http://systems.digital.nhs.uk/infogov/iga/resources/rmcop/index_html

Use of Personal Information

Clinical Commissioning Groups (CCGs) have no right of access to confidential patient information. Underpinning this legal position is the common law duty of confidence, and its interfaces with the Data Protection Act and Human Rights Act.

This means that Personal Confidential Data cannot lawfully flow from providers or GP practices directly to CCGs unless:

- There is a legal basis to do so

- There is explicit consent from the patient for the information to be shared. This needs to be explicit consent for a particular piece of personal data, being shared with an identified receiver for specific stated purpose.

- There is a need for sharing information for the direct clinical care

Personal Confidential Information must only be accessed by staff with authority to do so and when there is a legitimate need to do so. Processes are in place for random audits of legitimate accessing of Personal Confidential Information systems. Any discrepancies will be addressed in a timely and appropriate manner. If any inappropriate access is identified then appropriate HR processes will be used to address the issues.

Pseudonymisation

The Data Protection Act, Human Rights Act and the common law duty of confidence require that the minimum personal data are used to satisfy any particular purpose and patient level data should only be used for direct patient care.

If you are establishing a new information system or data collection tool or have any concerns regarding Personal Confidential Data with a system that you are using then please contact the Information Governance Officer who will be able to advise you of the Pseudonymisation arrangements we have in place.

Disposal of Personal Information

1. Do not use un-shredded personal information as scrap paper

2. Personal and confidential information must be put in confidential waste bins to be shredded

3. For destruction of computer-held information i.e. old hard drives or backup tapes you must consult the IT Department - do not leave lying around. Lock the equipment away

Privacy Statement

Walsall CCG has a responsibility to inform patients and staff how their information will be used. There is a privacy statement/Fair Processing Notice on the internet page stating that we do not collect any personal information about those using the site or use cookies to track or log information about users. Information submitted to the organisation will not be passed onto third parties and will only be used for the purpose that it was received or collected.

Portable Media

1. You should only use NHS approved pre-encrypted forms of portable media i.e. USB sticks, encrypted laptops

2. Encryption should be in line with NHS Guidelines

3. Never share or leave your password where others may find it

4. Portable media should be kept securely when not being used i.e. locked away

Post

Internal

1. Check recipient is still located at previous address

2. Include name, Job Title, Department and Base on the envelope

3. Ask for acknowledgment of receipt of post if required

4. Mark envelope private and confidential if necessary

5. Put personal information in envelopes

External

1. Make sure the envelop is correctly addressed

2. Does it need to be marked private and confidential

3. Should it be sent recorded delivery?

Personal Data Flows

Consider the following:

1. Am I authorised to collect this information?

2. Is it creating a new data flow and should it be registered with the organisation?

3. Never talk about patients or members of staff personal information unless it is justified by work requirements and never in places you can be overheard

Caldicott Principles

1. Justify the purpose of using confidential information

2. Only use it when absolutely necessary

3. Use only the minimum that is required

4. Access should be on a strict need to know basis

5. Everyone must understand their responsibilities

6. Understand and comply with the law

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

NHS Number

1. The NHS number is always to be used as the key identifier if a patient needs to be identified in all correspondence, communication or documentation including verbal

2. If non health partners communicate patient information then any response must clearly identify the NHS number and ensure all further correspondence use only that as the patient identifier

3. The NHS number must be used on all individual communication with a patient

4. Contact the information governance lead if you do not know the patients NHS number

5. All information systems that use patient identifiable information must use the NHS number as the principal identifier and no system can be procured if it is not compliant with the NHS number principles.

Subject Access Requests

Subject Access Requests will be very rare, as Walsall CCG does not hold many patient records however it may be applicable for complaints, investigations, staff records or research.

1. If a request is made then contact the information governance lead

2. Make sure that you record contact details of the requester

Freedom of Information Act 2000 (FOI)

1. Anyone can receive an FOI request and the request must be accepted

2. The request must be emailed to walsallccg.foi@nhs.net within 24 hours of the request being received

3. To comply with the Act the requester must receive the requested information (or reasons why the information can't be released) within 20 working days of the initial request

Sending Information outside the European Economic Area (EEA)

1. Check that the information needs to be sent outside the EEA with the Information Governance Lead.

2. Always check that the organisation you are sending the information to will adhere to the United Kingdom's Data Protection Act (DPA) 2018. If the organisation refuses

to comply with the DPA then the information is not to be sent. Please create a log of all information that is sent outside of the EEA

3. A contract or signed agreement will be needed to ensure the organisation agrees to adhere to the DPA 2018 and compliance with the contract will need to be monitored

4. Data subjects should be informed that their information is being sent outside the EEA and be given the right to withdrawn their consent.

Reporting an Information Governance Breach

1. If for whatever reason there is a breach in the information governance policies or procedures, please contact the Information Governance Officer as soon as you become aware

2. We must report a breach within 72 hours to the Information Commissioners Offices

Key Contacts

1. Caldicott Guardian, Dr R Mohan rajcholan.mohan@nhs.net

2. Senior Information Risk Owner tony.gallagher1@nhs.net 01922 618373

3. Head of Corporate Governance sara.saville@nhs.net 01922 603078

4. Corporate Governance Officer serena.ellis2@nhs.net 01922 618318

5. Data Protection Officer dataprotection.officers@nhs.net

Key Policies

- Information Governance Policy
- Staff Code of Conduct on Confidentiality
- Freedom of Information Policy
- IM&T Policy – Currently under review
- Corporate Records Policy
- Safe Haven Policy
- DH Non Health Records Retention Schedule
- Information Governance Strategy
- Subject Access Request Policy
- Information Governance Management Framework
- Information Security Policy – Currently under review
- Acceptable Use Policy – Currently under review

These policies are available from reception at Jubilee House 01922 618388 and from the intranet.