Joining up patient care through technology
eHEALTH Cumbria

Cumbria Partnership NHS
NHS Foundation Trust

e-Health Cumbria

INFORMATION GOVERNANCE

STAFF HANDBOOK AND CODE OF CONDUCT

TABLE OF CONTENTS

1. INTRODUCTION

This handbook has been produced to provide staff with all the necessary information required to abide by Information Governance legislation and national and local guidance. All Cumbria Partnership Foundation Trust (CPFT) Information Governance policies and procedures and information leaflets can be obtained from the Information Governance Team, based in Carlisle (see contact details) and on the intranet.
NB This booklet equally applies to those organisations who receive Information Governance advice and support through a Service Level Agreement.

2. INFORMATION GOVERNANCE

Information Governance is EVERYONE'S responsibility.

Information Governance is an 'umbrella term' linking together the approach and methods which the Trust uses to protect the data that it holds. It encompasses a set of key principles that staff must practice to strike a balance between using data effectively and protecting it.

IG is to do with how NHS / Social Care organisations and individuals handle Information

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. Better care for patients and improved healthcare for everyone depends on the availability of good information which is accessible when and where it is needed. The Trust's commitment to maintaining a high standard of information governance is outlined in the Information Governance Policy
The purpose of the Information Governance Policy and Framework is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. It is our approach to:

- Openness
- Legal compliance
- Information Security
- Quality assurance

The Trust is required to monitor its compliance with these areas through the Information Governance Toolkit
An assessment of compliance is completed in July (baseline), October (mid-year) and at the end of March (end of year). The Trust has put in place an Information Governance Performance Framework to support on-going improvement to meet its aspiration of a Level 3 compliance Trust

3. WHAT DO YOU NEED TO KNOW ABOUT INFORMATION GOVERNANCE?

Everyone who works in health or social care must be aware of the following:-

- the importance of the information we hold
- the legislation, guidelines and best practice for looking after such important information
- the responsibilities for obtaining, recording, using, keeping and sharing information

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and that they comply with them on a day to day basis. Managers are also responsible for promoting Information Governance standards and ensuring compliance by their team members.

Information Governance is not just about person identifiable data there are legal requirements on the Trust to manage corporate data such as policies, committee papers and plans appropriately, as under the Freedom of information Act 2000. The Trust is obliged to be open and accountable about its activities particularly related to the use of public funds

4. SENIOR INFORMATION RISK OWNER

Michael Smillie, Director of Strategy and Support Services is the Senior Information Risk Owner (SIRO) who takes overall ownership of the organisation’s Information Risk Policy, acting as champion for information risk on the Board and provides written advice on the content of the organisation’s Statement of Internal Control in regard to information risk.

For Cumbria Clinical Commissioning Group employed staff this role is undertaken by Charles Welbourn.

5. CALDICOTT GUARDIAN

Caldicott Guardians were introduced in 1997 following a report commissioned for the Government by Dame Fiona Caldicott to review the security and confidentiality of patient identifiable information in the NHS. The report outlined the weaknesses in the way the NHS handled confidential data and made a number of recommendations including the appointment of Caldicott Guardians.
The Caldicott Guardian is the person who makes the final decision on how, what, when and why personal identifiable information will be used in the organisation and how it will be received / sent by the organisation.

Dr Andrew Brittlebank, Medical Director is the Caldicott Guardian for the Trust

For staff employed by Cumbria Clinical Commissioning Group this role is undertaken by Dr David Rogers, Medical Director.

Following a request from the Secretary of State for Health, Dame Fiona Caldicott carried out an independent review of information sharing to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care.
The report was released in 2013 and makes 27 recommendations for improvements/changes on how information is shared in the Health and Social Care system and also introduces a **new 7th Caldicott Principle**.

The Seven Caldicott principles are:

- ✓ Justify the purpose(s)
- ✓ Do not use patient-identifiable information unless it is absolutely necessary
- ✓ Use the minimum necessary patient-identifiable information
- ✓ Access to patient-identifiable information should be on a strict need to know basis
- ✓ Everyone should be aware of their responsibilities
- ✓ Understand and comply with the law.
- ✓ The duty to share information can be as important as the duty to protect patient information

Before you handle, disclose or release any confidential information you should use the Caldicott principles as a guide to inform your decision. If you remain unsure contact your Line Manager in the first instance or the Information Governance Team for advice

6. CONFIDENTIALITY

All staff have a common law duty of confidentiality to protect person identifiable information. Managers must ensure that their staff are aware of and understand their obligations to conform to standards outlined within the NHS Code of Practice for Confidentiality. They are also responsible for ensuring their staff are notified of any changes.

6.1 An Overview of the Code of Practice

A duty of confidentiality arises when one person discloses information to another (e.g. Patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
It

- is a legal obligation that is derived from case law;
- is a requirement established within professional codes of conduct; and
- must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

Patients entrust us with, or allow us to collect, information relating to their health and other matters as part of their care and treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule, described later in this document, but non-disclosure in an identifiable form, applies in most circumstances.

6.2 Disclosing and using confidential patient / personal information

It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. In particular they should be informed of clinical governance and clinical audits, which are wholly proper components of healthcare provision. Patients should be informed that their information needs to be shared between members of care teams and between different organisations involved in healthcare provision. Consent to sharing should be obtained from the patient. This is particularly important where disclosure extends to non-NHS bodies.

6.3 Patient Consent to Disclosing

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed, and it must be quite clear that they understand the implications if their decisions about disclosure impact on the provision of care or treatment.

Where patients have been informed of:

- the use and disclosure of their information associated with their healthcare;

and

- the choices that they have and the implications of choosing to limit how information may be used or shared

then it is the responsibility of the clinician to document that the patient has been informed and fully understands the impact of their decisions. Discussions should be supported with an information leaflet

6.4 Information sharing with other agencies

It may be necessary for essential personal information to pass between the NHS, Local Authority, Social Services and other services. This may happen for example where one of these services is contributing towards a programme of care. To enable patients and service users to have confidence in the information that is held about them the Trust has developed documentation and protocols for information sharing. Agreements are held between the principle organisations involved in sharing.

A formal record must be kept by the relevant agency as to the reason why a disclosure of personal information was made. Where public interest is the reason, the grounds for doing so should be documented.

Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely

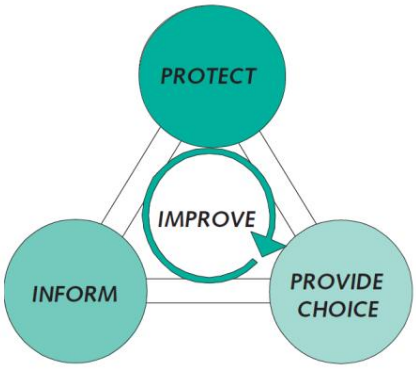
In deciding the most appropriate way to share personal information and the level of security required, you must always take into consideration the sensitivity of the information and the urgency of the situation, i.e. **take a risk based approach to determining appropriate measures.** If you are unsure of how to share information securely you should consult your manager.

Information sharing agreements are held by the IG Team.

6.5 The Confidential Model

The model outlines the requirements that must be met in order to provide patients with a confidential service. Record holders must inform patients/clients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures.

Figure 3 – Confidentiality Model



These processes are inter-linked and should be on going to aid the improvement of a confidential service. The four main requirements are:

PROTECT – look after the patient's information;
INFORM – ensure that patients are aware of how their information is used;
PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways.
To support these three requirements, there is a fourth:
IMPROVE – always look for better ways to protect, inform, and provide choice.

7. INFORMATION QUALITY ASSURANCE

Good quality information underpins sound decision making at every level in the NHS. Most importantly it contributes to the improvement of the service provided.

CPFT believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes

Think
CARRAT!

Complete
Accurate
Relevant
Reliable
And
Timely

8. INFORMATION SECURITY MANAGEMENT

The purpose of Information Security is to preserve the Confidentiality Integrity and Availability of information:

- Confidentiality – Data access is confined to those with specific authority to view the data and can be managed through passwords, smartcards etc.
- Integrity – Data is accurate and up to date and systems operate according to their specification
- Availability – data is available when required by those who have a right to access it

All records containing personal information whether they are kept in paper files or stored electronically must be secure. This can be achieved by following the guidance in the Information Security Policy, and E-mail and Acceptable Use Policy.

8.1 Smartcards

Access to person identifiable information should be strictly controlled. The most secure and safe way to do this is with an NHS smartcard. The card is used to determine who has access to a patient's record, and which parts of that record can be seen.

NHS smartcards are issued by the Registration Authority, who administer the registration process and ensure that Government security standards are upheld. The Registration Authority registers individuals; issues cards and provides support to card users.

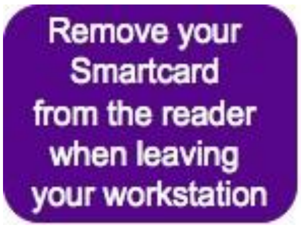
The Smartcard service for CPFT staff is provided by the Registration Authority which is based at Maglona House, Kingstown, Carlisle.

Staff should always keep their smartcard safe and use it appropriately. They must:

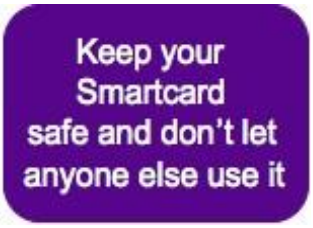
- ✓ Treat their smartcard like their credit or debit card and keep it in a safe locked place, separate from their passcode when not in use.
- ✓ Never allow anyone else to use their smartcard or use their PC whilst their smartcard is logged on to that PC.
- ✓ Never write down their passcode anywhere or share it with anyone.
- ✓ Never leave their smartcard unattended or in the smartcard reader when you are not actively using it.
- ✓ Report the loss, theft or damage of their smartcard immediately to their Sponsor and local Registration Authority so they can cancel their card and replace it as soon as possible, and complete an incident report form.
- ✓ Read, understand and sign the declaration on the RA01 form to agree their responsibility

Access through clinical systems to patient identifiable information is on a need to know basis and accessing records unless the user has a legitimate reason will be viewed as a breach of confidentiality.

If smartcard misuse by a staff member is discovered, the smartcard will be cancelled centrally and disciplinary action will be taken.



Remove your Smartcard from the reader when leaving your workstation



Keep your Smartcard safe and don't let anyone else use it

8.2 Access to the Trust's Network

Password access is the main security method for accessing the Trust's network

- ✓ Staff should take some care to construct a password i.e. something easy to remember but something not obvious for others to guess
- ✓ When a password is changed it must contain a mixture of characters from **each** of the following three categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
- ✓ The password must contain at least 8 characters.
- ✓ If a memory jogger is needed, write down a trigger word, not the password itself
- ✓ Passwords should never be kept with or near your laptop/USB/PC
- ✓ Avoid re-using or recycling old passwords. Your previous 10 passwords cannot be re-used
- ✓ Change passwords at regular intervals, and also if there is any indication of a possible system or password compromise
- ✓ Use password protected screensavers when away from your desk (activated by pressing Ctrl+Alt+Delete then select lock this computer)

NEVER SHARE YOUR PASSWORD

8.3 Your Work Environment

- ✓ Ensure that filing cabinets containing confidential information are always kept locked when not in immediate use
- ✓ Ensure filing cabinets are not sited in areas that are accessible to members of the public / visitors
- ✓ Ensure regular housekeeping of your files
- ✓ Remember to lock and secure the office when it is unattended and at the end of the day
- ✓ Whenever possible escort visitors at all times
- ✓ Remember to wear your identity badge
- ✓ Adopt a Clear Desk Policy - This a legal requirement of the Data Protection Act 1998, do not leave confidential information unattended or out overnight – particularly important when hot- desking or working in an open plan office

8.4 Disposal of Waste Paper

- ✓ Make sure that you dispose of confidential information appropriately in the confidential bins, i.e. lockable aluminium containers with "one way" letter box openings.
- ✓ The Trust's approved contractor is currently '**Shred-it**'.
- ✓ Always take care when putting anything in the bins, it cannot be retrieved!

8.5 Overheard Conversations

Where conversations are conducted by staff relating to the organisation's business either over the telephone, face to face or in the close proximity of public/reception areas, care must be taken that personal information is not overheard by persons who do not have a right or need to hear such information. Where departments or practices feel there is a definite problem, procedures should be implemented to improve the situation.

8.6 Sharing Your Outlook Calendar

To allow access to / share your Outlook calendar, in a safe and secure way, with other colleagues, you must use the Share Calendar option within your own Calendar. Always identify patients by their initials in your calendar, this allows colleagues who have access, to know where you are, whilst at the same time minimises the risk of a breach of confidentiality

9. HANDLING INFORMATION

9.1 Faxing Information

- Be aware of safe haven guidelines for confidential information
- Telephone the recipient and ask them to wait by the fax machine whilst you send the document
- Ask them to acknowledge receipt, check the number dialled, and check again before sending
- Where possible use pre-stored numbers

9.2 Communication via Text

Although it may be desirable to communicate with patient groups in this way there are potential information security risks that should be considered before you do so.

This must only be done with the express permission of the phone holder and should be revalidated regularly. Ensure that patients are fully informed of the risks and obtain their consent to the process (This should be evidenced either in writing using a signed consent form or noted on the clinical system)

Note: providing a mobile phone number does not constitute consent to use the number for text messaging.

Think:

- Are you confident that the person using the recipient mobile is the person to whom the message is intended?
- Can you be sure that you are using the correct phone number?
- Can you be sure that the patient has received the message?

Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) – as mobile phones are easy to misplace or may get stolen there is a danger of a breach of confidentiality occurring that the patient may find embarrassing or damaging. Mobile phone networks may be open to additional risks of eavesdropping or interception.

If you decide to go ahead with this method of communication, you should ensure you send the minimum amount of confidential data possible. For example, appointment reminders would comprise of the date and the hospital/surgery name, not the name of the patient or specific clinic.

9.3 Communication via Post

Ensure that envelopes containing personal identifiable information sent via internal or external mail are clearly and correctly addressed, marked 'confidential' and the senders address included.

9.4 Transporting Health Records

Refer to the Health Records Retrieval and Tracking Procedure available on the intranet for advice and guidance on transporting Health Records

- Adhere to the information on transit procedures
- Remember that the sender is responsible for what happens to this information in transit and until it has been returned to its safe store or is destroyed or disposed of correctly

9.5 Printing and Photocopying

- ✓ Keep the number of copies to a minimum
- ✓ Photocopying machines should be sited in areas where the general public do not have physical access.
- ✓ Remove papers from the glass after copying.

9.6 Removable Media

- Staff and contractors are not permitted to introduce or use any removable media other than those provided or explicitly approved for use by Cumbria Partnership Foundation Trust.

- Removable media includes tapes, floppy disks, removable or external hard disc drives, optical discs, DVD and CD-ROM, cameras, video cameras, solid state memory devices including memory cards and pen drives.

- Staff must be authorised to use removable media for the purposes of their job roles by an appropriate manager and are responsible for the secure use of the removable media and must ensure that it is physically protected against loss, damage, abuse or misuse when used, stored and whilst in transit.

9.7 Laptops

All laptops are encrypted for safe use.

- ✓ Confidential information should not be stored on the hard drive;
- ✓ Laptops should be locked away in a draw or cupboard when not in use;
- ✓ Never leave the laptop on show in your car
- ✓ Ensure regular housekeeping of laptop files.
- ✓ Ensure you log onto the network at least every 30 days. This ensures the anti-virus is up to date
- ✓ Trust IT equipment is not covered by the NHS insurance scheme and you may be held fully or partially liable for any loss, damage or theft occurring to Trust IT equipment whilst in your care.

9.8 Memory Sticks

These devices fall under the local Information Security Policy in that they must be password protected and encrypted. Staff must not use personal USBs for work purposes under any circumstances. For further information, please refer to the Information Security Policy and Mobile Media Policy.

9.9 Working Papers and Message Books

When not in use, paper-based information should always be kept in folders, envelopes or other containers which prevent sight of the content, and be locked securely away. It must not be left in an in-tray or on the desk. To minimise loss of information and reduce storage space Staff are advised to work in a paper light / paper-less manner.
When using a Message Book it should be kept away from public view in an environment with no public access. At the end of the working day it must be stored in a secure location. Sensitive patient identifiable information should not be recorded in message books.

9.10 Answer Phones

Answer phones receiving personal information must have the volume lowered so that the information is not being un-necessarily overheard.

You must only leave a message on a patient or individuals answer phone if it is urgent and/or you have prior permission from the patient or individual. If this is the case, leave your name and number only – do not say it is the hospital/surgery calling. Never leave any person identifiable information within the message.

9.11 Cameras and Video Cameras

Photography and video recordings are a valuable part of assessing and evidencing a patient's condition. Refer to the Photography and Video Recording Policy and Procedures for specific guidance

9.12 Other Electronic Media

- A Digital Dictation Solution is available to replace antiquated tapes and dictation machines.
- Thermal Ribbon Cartridges from certain fax machines must be disposed of by formal confidential waste disposal means, because of the imprint of the content left on the ribbon
- Any unwanted IT equipment e.g. PCs, Blackberries etc. must be disposed of via the IT Department. Contact the e-health service desk for advice.

9.13 Email

9.13.1 Sending emails internally

Person identifiable information can be sent securely across the local email exchange network to the following organisations:-

1. North Cumbria University Hospitals NHS Trust
2. Cumbria Clinical Commissioning Group
3. University Hospital of Morecambe Bay

- However, in accordance with our email policy, if the email is being sent within the Cumbria NHS Community of Interest Network ("CoIN") (e.g. xyz@ncuh.nhs.uk to abc@cumbria.nhs.uk) and via NHS mail (e.g. cde@nhs.net to uvw@nhs.net) you can send person identifiable information as an attachment but it must be password protected.

- Person identifiable information must not be put in the main body of the email or in the subject header. If for any reason an email needs to be sent where there is no attachment then only the NHS number should be used.

- All attachments containing personal identifiable information must be protected with a password.

The Trust has been working hard to implement end to end encryption which allows emails to be sent securely to organisations both within and outside the NHS without the need to use NHS mail accounts. This is seen as the preferred option for the Trust as it will allow information to be sent securely by email to organisations which do not have NHS mail accounts (e.g.. solicitors, etc.).

If you need to send highly sensitive information in this way then contact the Information Governance team regarding the possibility of an encryption licence. You will need to Map your flows of information first to see whether this is the best route for you.

9.13.2. Emailing Cumbria County Council – Adult Social Care and Children's services

A secure email link is in place. Emails can be sent securely from an nhs.uk address to someone with a cumbria.gov.uk address but attached documents should be protected with a password

9.13.3. Emailing Other Organisations outside the NHS

Emails containing person identifiable information must not be sent to non NHS organisations outside the local email exchange network. Contact the Information Governance Department for advice on sending person identifiable information to an organisation outside the NHS.

9.13.4. Guide to Emailing

The following email chart can be used as a reference point along with the notes provided. If you need further advice please contact the IG Team: information.governance@cumbria.nhs.uk

PID EMAIL CHART	CPFT	CCG	UHMB	NCUH	GP's (Centralised Email Server)	Cumbria County Council	GP's (Local Email Server)	NHSmail	Greater Manchester West	NHS Property Services	NECS	Northumbria Healthcare NHS Foundation Trust	NHS England	North Lancashire	Others
CPFT	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗
CCG	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗
UHMB	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗
NCUH	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗
GP's (Centralised Email Server)	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗
Cumbria County Council	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
GP's (Local Email Server)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
NHSmail	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Greater Manchester West	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
NHS Property Services	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
NECS	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
Northumbria Healthcare NHS Foundation Trust	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
NHS England	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
North Lancashire	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗

PID - Risk, use encryption	Seek advice and use approved encryption products, Voltage, AES 256 etc.
PID - Aware, zip data or anonymise	Password protect, anonymise and follow up with phone call
PID Safe - take normal patient confidentiality precautions	Ensure that you comply with normal patient confidentiality (i.e. basic password protect)

NB: PLEASE NOTE
Centralised Email Servers: GP practices using these servers are classed as internal, please see coding in above matrix.

GP Local Servers: These practices (detailed below) are classed as 'external' organisations for the purposes of emailing and more robust precautions are required:
Brunswick House, Dalston Medical Practice, Grosvenor House, Solway Health Services (Maryport), Silloth Medical Practice and St Paul's Medical Centre

10. INCIDENT REPORTING

An incident is any event, which has resulted in, or could result in:

- The loss, theft or disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or data being put at risk
- An adverse event, for example:
  - ✓ Embarrassment to the NHS
  - ✓ Threat to personal safety or privacy
  - ✓ Legal obligation or penalty
  - ✓ Financial loss - for any suspected fraud - refer to the counter fraud policy on the intranet
  - ✓ Disruption of activities.

All incidents or information indicating a suspected incident should be reported as soon as possible to your line manager. Details of incidents must be reported via the organisations' risk incident reporting procedure using Ulysses (the process for risk management).

The Ulysses system allows us to collate information about the number of incidents being recorded across the organisation. By looking in detail at the collected information we can learn from things that go wrong and work to make it a safer place for both our patients and our staff.

The incidents should be reported using category ‘Information Governance'. The Information Governance Team are alerted to these incidents and will support the investigation being undertaken by the incident manager where appropriate.

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as a Serious Untoward Incident (SUI).

For further details please see the Serious Untoward Incident Policy available on the intranet

11. RECORDS MANAGEMENT

All staff have a responsibility to manage records effectively. Poor records management can lead to inefficiencies in service, inappropriate disclosure of information and in the worst cases, can impact on clinical care.

All staff have a contractual obligation to maintain good records management. Those with a professional registration are also required to maintain good record keeping as part of their registration. The Trust is subject to compliance regimes, in particular ‘outcome 21’ of the Care Quality Commission regulations, where failure to meet regulations can result in fines and other penalties.

The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

Guidance on Records management both Health and Corporate records is available on the intranet.

The key things to remember about managing any record are:

- To file it appropriately - work with colleagues to agree filing systems so that you all know where to find things.

- Mark records appropriately - if they contain confidential information then 'mark' the record as such. This is an indicator to others that disclosures should be carefully considered. It shouldn't be taken as an absolute rule not to disclose data.

- Consider when records are no longer used - do they need to be archived for a period of time? If not, they must be disposed of in line with Trust guidelines.

12. DATA PROTECTION ACT 1998

Personal data must be collected lawfully and correctly. Each NHS organisation must comply with the Data Protection Act 1998 (DPA). The Data Protection Act defines 8 Principles. The following guide provides a summary of these principles and highlights areas for consideration to ensure compliance.

Data should be

1. **Processed fairly and lawfully** - There should be no surprises and you should always inform data subjects why you are collecting their personal information and what you intend to do with it and who you might be sharing it with.

2. **Obtained/ processed for specific lawful purposes** - Only use the personal information for the purpose for which you obtained it. – Consider why you been given this information. Are you processing it only for the reasons it has been given to you?

3. **Adequate, relevant and not excessive** - Only collect and keep the information that you require. Do not collect information 'just in case'.

4. **Accurate and kept up to date** -Always ensure accuracy of the data you are recording. Check that you are capturing the most current information.

5. **Not be kept for longer than necessary –** Consider how long the information should be kept. Ensure that it is disposed of appropriately when finished with and follow the Trust's retention guidelines which are available on the intranet

6. **Processed in line with the rights of data subjects** - Is the data being processed according to the subject's wishes?

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.** Is the data held in a secure environment?

8. **Not transferred outside European Economic Area (EEA) without adequate protection** - If there is a need to send personal identifiable information in a computer readable format outside the UK you must discuss this with the Information Governance Team to check if any further legal requirements apply. Ensure consent is obtained and information is in a tamper proof envelope if sending outside EEA.

12.2 Data Protection Act 1998 – Definition of Personal and Sensitive Information

Personal data is information held by an organisation that can identify a person (the data subject). It could be a patient, a member of personnel (past, present and prospective) or a supplier contractor. It can be recorded on paper manually, computerised, electronic or digitally (CCTV & identifiable voice recordings are also included).

Personal Information: Name, DOB, address, postcode, NHS No., NI No., next of kin details, carer's details and bank details.

Sensitive Personal Information: For example

- ✓ Health or physical condition,
- ✓ Trade Union membership,
- ✓ Sexual orientation and sexual life,
- ✓ Ethnic origin,
- ✓ Religious beliefs political views,
- ✓ Criminal convictions.

12.3 Data Protection Act 1998- Subject Access Request

The Act allows certain rights to subjects, (the person whose data has been collected). The most common request in the NHS is the right of subject access, the right to know what personal information is on a computer or in manual records held by the organisation. More often than not this is a request to view or have a copy of their medical record.

All staff should know the details of the appropriate person who deals with these requests, as they must be dealt with in a specific manner. The DPA states that a request must be processed within 40 calendar days but the Department of Health states that the NHS should endeavour to respond within 21 days. If the Trust fails to meet this deadline then the data subject has the right to complain to the Information commissioner who may respond with an "improvement notice" to the Trust.

Requests must be made in writing. Every request is logged and challenged to ensure that only the correct person (the data subject or their designated representative) views or receives the requested personal information. Subject Access Policy and Procedures for dealing with these requests are both available on the Trust's websites.

Subject access requests should be sent to AccesstoRecords@cumbria.nhs.uk

13. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland
Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings
The Act does not give people access to their own personal data (information about themselves) such as their health records
Request for information should be made to FOIrequest@cumbria.nhs.uk

13.1 FOI Exemptions

A requester may ask for any information that is held by a public authority. However, this does not mean the Trust is always obliged to provide the information. In some cases, there will be a good reason why it should not make public some or all of the information requested.
An entire request can be refused under the following circumstances:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

In addition, the Freedom of Information Act contains a number of exemptions that allows the Trust to withhold information from a requester. In some cases it will allow you to refuse to confirm or deny whether you hold information. Some exemptions relate to a particular type of information or the harm that would arise or would be likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests More details can be found in the Freedom of Information Policy

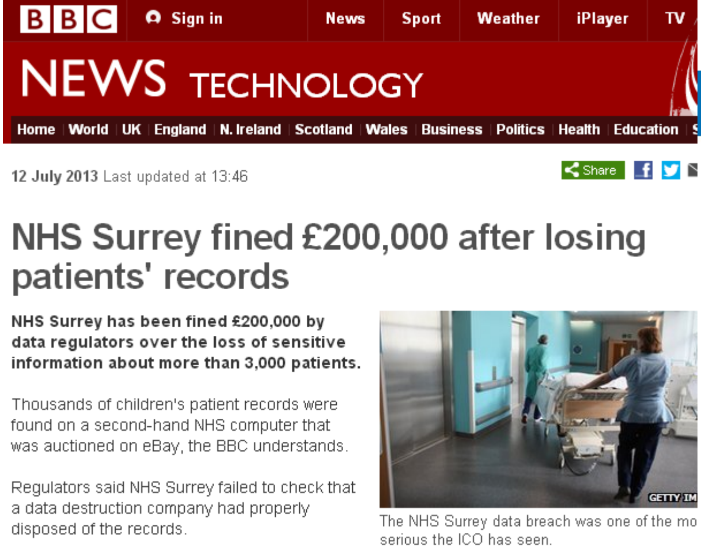
13.2 Publication Scheme

As well as responding to requests for information, Trusts must publish information proactively. The Freedom of Information Act requires every public authority to have a publication scheme, approved by the Information Commissioner's Office (ICO), and to publish information covered by the scheme.
The scheme sets out our commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information.
The Trust publication scheme is available on the intranet

The Trust's FOI Lead is Yvonne Salkeld, Head of Information Governance

14. THE INFORMATION COMMISSIONER

It is the Information Commissioner's function to ensure compliance with the Freedom of Information Act, the Data Protection Act and Environmental Regulations. The Information Commissioner's Office has the power to issue enforcement notices, financial penalties up to £500,000 and if needs be, initiate court proceedings to ensure compliance



12 July 2013 Last updated at 13:46

NHS Surrey fined £200,000 after losing patients' records

NHS Surrey has been fined £200,000 by data regulators over the loss of sensitive information about more than 3,000 patients.

Thousands of children's patient records were found on a second-hand NHS computer that was auctioned on eBay, the BBC understands.

Regulators said NHS Surrey failed to check that a data destruction company had properly disposed of the records.

The NHS Surrey data breach was one of the mo serious the ICO has seen.

15. COMPLIANCE REQUIREMENTS

The organisation is obliged to abide by all relevant European Union legislation. Staff should be aware of the following legislation and NHS guidance:

- Data Protection Act
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- Human Rights Act 1998
- Confidentiality: NHS Code of Practice
- Information Security Management – ISO27001
- NHS Code of Practice – Records Management
- Information Quality Assurance

16. THE INFORMATION GOVERNANCE TEAM

For any queries concerning the information in this Code of Conduct contact the Information Governance Team

Maglona House
68 Kingstown Broadway
Carlisle
CA3 0HA

Email Address: information.governance@cumbria.nhs.uk

Freedom of Information Act requests to FOI@cumbria.nhs.uk

Access to Records Requests at accesstorecords@cumbria.nhs.uk

Registration Authority service at: CPFTsmartcard@cumbria.nhs.uk

NOTES