Welcome to the RBCH eLearning module

Information Governance and Record Keeping

Authored by:

Camilla Axtell
Information Governance Manager - Royal Bournemouth & Christchurch Hospitals

Learning Outcomes

By completing this module you will find out about:

- confidentiality law and guidelines - what they are and how to avoid breaching them
- how to comply with Data Protection and Freedom of Information legislation
- good record keeping
- effective information security
- how to find out more.

What is Information Governance?

Information Governance (or 'IG') is a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information.

IG applies to all the types of information which the Trust may process, but the rules may differ according to the type of information concerned.

Information Governance features prominently in UK law and constitutes the following:

- Confidentiality
- Data Protection Act 1998
- Freedom of Information Act 2000
- Records Management
- Information Security
- Best Practice Guidance
- Annual IG Toolkit Assessment.

"Every citizen should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. ***Everyone*** *working in the health and social care system should see Information Governance as part of their responsibility."*

What is information?

The tabs below describe more details on what we mean by information.

Personal
name, date of birth, home address, demographic details covered by the Data Protection Act 1998.
Sensitive
ethnicity, disease, medical condition, sexual life covered by the Data Protection Act 1998.
Corporate
contracts for suppliers, minutes of meetings, financial information, policies covered by the Freedom of Information Act 2000.

Information is confidential if it meets three conditions; select the numbers below to see these conditions.

Condition 1

It is private information about you.

Condition 2

You gave it to someone who has a duty of confidence (in this case the doctor or staff who work on behalf of the doctor)

Condition 3

You expect it to be used in confidence

Confidential Information

The duty of confidence can be broken in special circumstances such as a need to protect the public e.g. serious crime, or to prevent abuse e.g. in relation to Safeguarding Children or Adults.

UK law says that health information is confidential.

Confidential Service

The legal basis for providing a confidential service to patients is known as the 'Common Law Duty of Confidentiality':

if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent

a duty of confidence arises when sensitive information is obtained and/or recorded in circumstances where it is reasonable for the subject of the information to expect that the information will be held in confidence

patients provide sensitive information relating to their health and other matters as part of their seeking treatment and they have a right to expect that we will respect their privacy and act appropriately. The duty can equally arise with some staff records, e.g. occupational health, financial matters

patients have a right to be informed about how we will use their information for healthcare, the choices they have about restricting the use of their information and whether exercising this choice will impact on the services offered to them.

Information Sharing and Consent

Information can sometimes be shared without seeking patient consent where this is in the overwhelming public interest, for example sharing information with the police which may help them apprehend an offender where they are investigating a serious crime (e.g. murder or manslaughter).

Statutory information

The Trust is required to share some information with other agencies, regardless of patient consent – for example, where an order of court exists for information to be disclosed, or sharing information about communicable diseases.

Best interests of patients

Information can be shared without seeking consent if it would be in the best interest of the patient, such as for making other relevant agencies aware of adult/child safeguarding issues, or where a patient lacks capacity to provide consent but the disclosure is required for their own wellbeing.

Information Sharing and Consent

When sharing information, in all cases first consider what information needs to be shared to complete a specific task – is using or disclosing personal information really necessary?

Personal information shared should be the minimum necessary and be anonymised or pseudonymised where possible if there is no need to disclose identifiable details.

All decisions taken to share or disclose information must be fully documented within the patients' medical records or staff personnel file. If unsure, you should seek further advice from the Trust's Caldicott Guardian or Information Governance Manager on whether it is appropriate to disclose information.

Information Sharing and Consent

In the course of your work you will come into contact with sensitive and confidential information, about patients and/or staff members – the fact that a person is a patient of the hospital is, in itself, confidential. Always remember confidentiality is a legal requirement for all staff, supported by the confidentiality clause in your employment contract and, where applicable, your professional code of conduct.
This includes not disclosing information inappropriately, keeping information safe and secure, and using information in accordance with the law and Trust policies.

Breaches of confidentiality may lead to disciplinary measures, and possible legal proceedings against the Trust or the individual staff member involved in the breach.

Caldicott Guardian

To help improve levels of confidentially throughout the NHS, a report was commissioned in 1997 by the Chief Medical Officer - the Caldicott Report.

One of the key outcomes of this report was that Caldicott Guardians were appointed in each NHS Trust, in order to safeguard access to patient-identifiable information.

The Caldicott Guardian is responsible for reviewing, overseeing and agreeing policies governing the protection of patient or personal information. The Caldicott Guardian also takes responsibility for overseeing organisational compliance with the Caldicott Principles.

Caldicott Principles

A key recommendation of the Caldicott report was that staff justify every use of confidential information and routinely test it against a list of principles. Never use or disclose confidential information if you would not be complying with any of the following Caldicott Principles:

- justify the purpose of using or disclosing information
- only use or disclose information if absolutely necessary
- use or disclose the minimum information necessary
- work on a need to know basis
- be aware of your responsibilities
- comply with the law

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

QUESTION

Read this **scenario** and then answer the question below.

Confidentiality Scenario

A famous celebrity is taken ill while performing at a local theatre. Appendicitis is diagnosed and the celebrity requires emergency surgery. Several hospital staff recognise the celebrity and some of them look up his case notes.

Following the surgery the anaesthetic practitioner rings a friend to tell them about this surgery and other information on this celebrity's past healthcare history. The following day the newspaper publishes details of the surgery and other health issues the celebrity has.

What actions were the staff members justified in doing?

☐ Viewing the celebrity's full medical history

☐ Looking up case notes after seeing that the celebrity was a patient

☐ Discussing with a friend the patient's previous medical history

How many did you answer?

.

All of the above are wrong. The patient is entitled to have his personal information kept confidential.

It is a breach of the Common Law Duty of Confidentiality, Data Protection Act 1998 and Trust policy to access patient information without a justifiable reason, and to share that information with those who have no reason to know.

Data Protection Act 1998

The Data Protection Act 1998 applies to all organisations in the UK that process personal information. The Act goes hand-in-hand with the common law duty of confidence and professional and local confidentiality codes of practice to provide individuals with a statutory route to monitor the use of their personal information.

A breach of one of the eight Data Protection Principles can result in legal action being taken against an individual and/or the organisation. Learning the Principles of the Data Protection Act is therefore very important.

There are additional offences under the Act of unlawfully obtaining, disclosing or selling personal data, which can result in a criminal conviction.

There are eight principles to the Data Protection Act 1998 that must be followed when handling personal information. Select the titles below to see more information.

Processed fairly and lawfully

Ensure that the proposed use of the information is lawful in the widest sense, e.g. doesn't breach other legal restrictions such as the common law duty of confidentiality. Inform patients why you are collecting their information, what you are going to do with it, and who you may share it with.

Processed for a specific purpose

- only use personal information for the purpose for which it was obtained.
- only share information outside your organisation, team, ward, department, or service if you are certain it is appropriate and necessary to do so.

If in doubt, check first.

Adequate, relevant, not excessive

- only collect and keep the information you need.
- do not collect information 'just in case it might be useful one day'. You cannot hold information unless you know how it will be used and it is a justified use.
- explain all abbreviations, use clear legible writing and stick to the facts – avoiding personal opinions and comments.

Accurate and up to date

- take care when entering data to make sure it is correct
- make sure you check with patients that the information is accurate and up-to-date
- check existing records thoroughly before creating new records and avoid creating duplicate records

Not kept longer than necessary

- follow retention guidelines set out by the Records Management NHS Code of Practice and the Trust's records management policies
- make sure your information gets a regular 'spring clean' so that it is not kept 'just in case it might be useful one day'
- dispose of information correctly, according to the Trust's disposal policy.

Processed in accordance with rights of data subject

Individuals, whether staff or patients, have several rights under the Act. In summary individuals have:

- the right of access to personal data held about them (known as a 'subject access request')
- the right to prevent processing likely to cause damage or distress
- the right to have inaccurate data about them corrected, blocked or erased
- the right to prevent processing of information about themselves for purposes of direct marketing rights in relation to automated decision-taking

The rights are not absolute, that means there may be occasions where the organisation is permitted to override them. Speak to the Trust IG Manager for more information.

Held securely

This requires that all organisations that process personal information have security measures in place to ensure that the information is protected from accidental or deliberate loss, damage or destruction.

The Trust has security policies and processes to ensure the security of personal information. There are also guidelines for staff about how to ensure personal information is protected from unauthorised access.

You must make sure you comply with all the security processes and guidelines so that access to personal information is only available to those authorised to do so, and information is not accidentally or deliberately lost, damaged or destroyed.

Some of the measures you should comply with are:

- only send confidential faxes using safe haven or secure faxes
- ensure confidential conversations cannot be overheard
- keep your passwords secret
- lock paper files away when they are not in use
- transport personal information by secure methods.

Not transferred outside EEA

- if sending personal information outside the European Economic Area (EEA), make sure consent is obtained where required and ensure the information is adequately protected.
- be careful about putting personal information on websites, which can be accessed from anywhere in the world - get consent first.
- check where your information is going, and know where your suppliers are based.

Freedom of Information Act

Would you know what to do if you received a written request from a patient asking for a detailed breakdown of your organisation's expenditure for the year?

The Freedom of Information (FOI) Act serves to make publicly funded organisations more open and accountable and requires organisations to make information routinely available to the public, either through the organisation's website or via responses to requests for information.

Anybody can make a request under the FOI Act, for which there is usually no charge.

- Documents such as policies, procedures, minutes of meetings and e-mails are all public records, and as such could potentially be disclosed under the FOI Act, if requested - be mindful of the content of documents that you create.
- It is a criminal offence to knowingly block or erase information that has been requested for disclosure under the FOI Act.
- Freedom of Information Act
- Select the tabs below for more information.

Types of information

The FOI Act gives the public the right to request any recorded information held by any type of public authority (including NHS Trusts) or held by persons/organisations providing services for those authorities.

The public can request information held within things like minutes of meetings, work emails, work diaries, corporate reports and other work documents. Exemptions may apply to some information, which therefore need not be disclosed.

Form of request

Requests for information must be made in writing but there is no need for the applicant to mention the FOI Act. If a patient or member of the public asks you for information that you think is covered by the FOI Act, you should ask them to put their request in writing or assist them to do so.

Processing requests

If you receive a request for information, you should promptly forward it to the person in the organisation that has been assigned responsibility for FOI requests – the Trust's Information Governance Manager. (foi@rbch.nhs.uk).

Response times

Generally, the organisation must comply with requests for information within 20 working days.

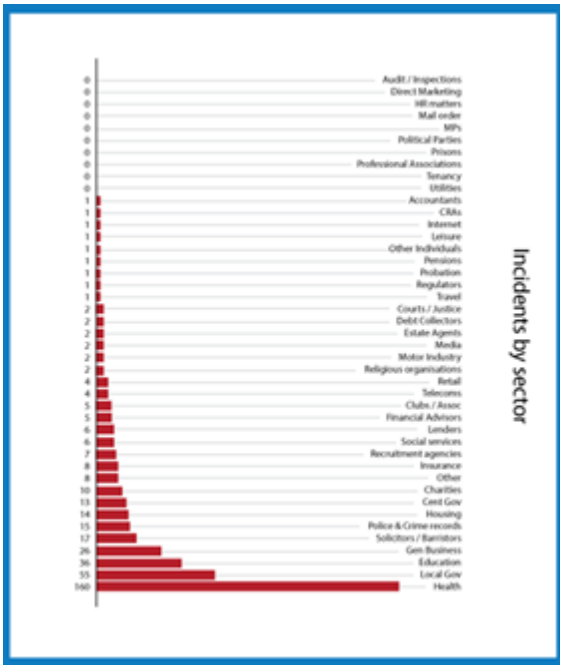
Exemptions

There are several circumstances under which information should not be disclosed – e.g., if the information can easily be obtained from elsewhere, if the organisation has already published the information or has firm plans to do so, if the information is confidential or if it is personal information. Unless you are the person nominated to respond to FOI requests, you will not have to take decisions on whether information should be withheld.

Relevance to NHS

The NHS is directly affected by Information Governance Law and it is particularly important that Trust employees and volunteers must abide by the correct policies and procedures.

- do you use e-mail or faxes?
- have you ever had or overheard a conversation about a patient or a member of staff?



- have you ever cleared out some old files?
- do you keep electronic or paper files?
- do you line manage staff?
- do you use the restaurant or walk through the hospital corridors?

Relevance to NHS

'Patient who was going to Pharmacy with her prescription asked by member of staff if she could also take prescriptions relating to a number of other patients with her.'
RBCH, January 2014
'Two ward handover sheets found on the ground in the Consultants' car park - contained significant amount of confidential and personally identifiable information about patients.'
RBCH, March 2014

Breaches

Report a breach of Information Governance via an **Adverse Incident Report** (AIR) form:

- breaches or potential breaches of confidentiality
- any loss or potential loss of personal/sensitive data
- any unauthorised access to systems
- malfunction of IT equipment that might affect patient care
- **anything that doesn't feel right.**

Breaches of Information Governance are equally as serious as any other incident which occurs within the Trust. Any breach of Information Governance guidelines, including near misses, should be reported via the Trust's AIRprocedure immediately.

All Information Governance incidents reported are copied to the Trust's IG Manager, and advice should be sought when investigating such an incident.

The Trust is obliged to report serious breaches of Information Governance to external organisations such as Monitor, the Department of Health and Information Commissioner's Office.

Implications?
- potential **£500,000** fine for the Trust
- criminal proceedings against staff.

Information Commissioner's Office (ICO)

- The ICO is the UK's independent public authority set up to uphold information rights by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.
- Examples include; 250 hard drives containing sensitive data stolen from hospital and sold on eBay (£325,000) and ex-employees pension records found in overflowing supermarket recycle bin (£250,000).
- The ICO has been granted powers by the government to fine organisations up to £500,000 for serious breaches of the Data Protection Act 1998. The ICO can also bring prosecutions against individuals for breaches of the Data Protection Act 1998.

How to Avoid Breaches

Emails

E-mails sent within the Trust (i.e., from an @rbch.nhs.uk e-mail address to an @rbch.nhs.uk e-mail address) are secure, however caution should still be used to ensure that information is sent to the correct recipient, and that only the minimum amount of information necessary is sent

Personal information should not be sent outside the Trust via e-mail unless the message is encrypted or sent using NHS.net from end to end, i.e. the sender and receiver must have an NHS.net e-mail address

Contact the IT Helpdesk for assistance with e-mail encryption

Fax

Do not fax personal or confidential information unless it is absolutely necessary. If it is necessary, ensure that you fax to a secure Safe Haven fax machine.

If faxing personal information:

- double check the fax number, including area code and whether an outside line is required
- ask the recipient to confirm receipt of the fax
- ensure you use a cover sheet, marked 'Private and Confidential' (do not include personal information on the cover sheet)
- where practical, personal details (e.g. name and address) should be faxed separately

Post

• ensure envelopes containing personal or sensitive material are secure and marked 'Private and Confidential'
• double check the full postal address of the recipient (including post code)
• ensure that no additional information is placed in the envelope in error, e.g., a letter for another patient
• if using window envelopes, ensure that the letter text is not visible through the envelope window
• choose a secure method for sending confidential information through the external post e.g. special delivery.
• ensure that incoming post is handled appropriately, including noting the date of receipt.

Access to Information

You may be granted access to medical or personnel records as part of your work.

It is a breach of Trust policy, and also a breach of the Data Protection Act 1998 and/or the Computer Misuse Act 1990 to obtain access to information with which you have no 'legitimate professional

relationship'. This includes accessing your own medical records, and medical records of friends, family, colleagues etc., unless for legitimate work purposes.

There are subject access procedures in place within the Trust for any staff member or patient to obtain access to their personal information.

Remember to always keep your password confidential and do not write it down.

Insecure storage, transportation & destruction of information

With regards to storage, transportation & destruction of information:

- ensure that filing cabinets containing confidential information are always kept locked when not in use
- do not leave personal information out in unoccupied areas accessible to the public
- ensure filing cabinets are not sited in areas which are not controlled and are accessible to members of the public/visitors
- remember to lock and secure the office when it is unattended and at the end of the day
- when disposing of office furniture (desks, filing cabinets etc.), ensure that they are cleared of all files prior to disposal

Insecure storage, transportation & destruction of information

With regards to storage, transportation & destruction of information:

- ensure that you wear your identity badge and do not lend your identity badge to anyone else
- do not share office access (keypad) codes with unauthorised staff, visitors or contractors
- confidential, personal and sensitive information should not be taken off site, unless authorisation has been granted.

Where it is necessary to take confidential information off site, **remember:**

- do not leave the information unattended
- only the minimum information required should be taken off site
- keep information secure at all times (e.g., do not leave in your car overnight).

- Insecure storage, transportation & destruction of information
- **Always** challenge unknown individuals attempting to access records.

Insecure storage, transportation & destruction of information

Be sure that you dispose of confidential information appropriately and securely, ensuring compliance with Records Management: NHS Code of Practice records retention schedules.

All personal information is confidential and must be shredded or disposed of as confidential waste using bulk waste (white) bags available through Commercial Services. Confidential waste paper must not be used as scrap paper for messages, notes etc.


ROYAL BOURNEMOUTH AND CHRISTCHURCH HOSPITALS NHS TRUST
BLOOD TRANSFUSION DEPARTMENT

BUTLER | LAURA | 6148071 | 01/01/10 | Female
KYH | Bournemouth General | A&E Dept.
O Positive
6.4305.9 | Issue Fridge 1 | ALL USED PACKS MUST BE PLUGGED AND RETURNED

10/03/06 RCALD O+ 0054 706 702 583 A
15/03/06 RCALD O+ 0054 706 115 064 V
16/03/06 RCALD O+ 0054 706 116 528 K

UNLESS BLOOD BANK HAS BEEN NOTIFIED TO THE CONTRARY THIS BLOOD WILL BE DERESERVED | 27/02/06

Units typed Kell negative and Rir by NBS.

22/02/06 20:03 24/02/06 SPJ

Record Keeping

'All individuals who work and volunteer for an NHS organisation are responsible for any records which they create or use in the performance of their duties… any record that an individual creates is a public record.'

Records Management: NHS Code of Practice

Without good quality information to work from, we cannot provide the highest quality of care to patients. It is therefore essential that the information that we record, hold and use is fit for this purpose.

Good IT practice

Remember:

- never leave a computer terminal unattended and logged-in
- always save files (particularly when they contain patient information) on network drives only – never on a C:\drive
- do not store personal data on mobile devices (other than short term needs)
- mobile devices must be encrypted and password protected
- only use authorised, Trust-owned equipment – neverpersonal equipment, such as USB sticks
- never share passwords or Smartcards with others
- comply with all Information Governance and IT Policies.