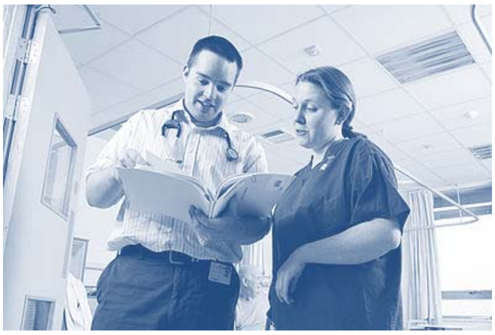
Royal United Hospitals Bath NHS
NHS Foundation Trust

Information Governance

Fact Sheet

Last Updated: November 2018
Produced by : Learning & Development and based on the Core Skills Training Framework

Developed with the Head of **Information Governance**



Local Guidance on:

- *Caldicott Principles*
- *Data Protection Act 2018*
- *Freedom of Information Act 2000*
- *Practical guidance*
- *Contact details*

This will help you complete your eAssessment

Please note:

there are limited attempts at the eAssessment (online quiz) which is available in ESR.

ESR
(via Smartcard)

Information Governance

This fact sheet aims to provide you with an update on the importance of maintaining data confidentiality and security. Further information can be found on the Trust intranet site or by completing the eLearning programme on ESR.

You might like to refresh your training with this factsheet if you are about to attempt the eAssessment. eAssessments are online tests and are a quick way to update your mandatory training.

Protect yourself

by getting trained

Staff who have been trained **have not been prosecuted** when making accidental breaches.

Recommended courses on ESR:

427 RUH Information Governance eLearning

427 RUH Information Governance eAssessment

There are eLearning and classroom options available for Information Governance training.

Information Governance & Caldicott Principles

Information Governance applies to the personal information of **living individuals;** in the NHS this can be staff or patients. In order to fulfil our duties to protect personal information we must follow the **Caldicott principles:**

1. Justify **the purpose** of using confidential information

2. Only use confidential information when **absolutely necessary**

3. Use the **minimum** confidential information required

4. Allow access to confidential information on a strict **need-to-know basis**

5. Understand your **responsibility** to protect confidential information

6. Understand and **comply** with the law

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

Overall responsibility for patient confidentiality sits with our Caldicott Guardian - Bernie Marden, Medical Director.

What does this mean in practice?

When obtaining, recording, holding or sharing personal information the law must be followed. For staff this means ensuring that;

- Patient information is **accurate and up-to-date**
- Only relevant information is shared with **relevant people**
- Information is **shared within the law** – see appendices
- **Access to information is restricted** to those who require access
- Information is **securely transferred, stored and disposed**

Staff responsibilities for good governance

All staff have a responsibility for information security. You must protect confidentiality and personal information, whether this be staff, patient or commercially sensitive information e.g board papers or contracts. This means that;

You SHOULD
• ensure your **passwords are complex** (upper and lower case, numbers and punctuation). They should not be written down and should be changed regularly.
• only use nhs.net email to send confidential information to **encrypted email** addresses (i.e nhs.net to nhs.net). Where identifiable information and data is to be provided to any other emails there is a secure encryption method that must be used and this is obtained from the IG team.
• only access the records of individuals with whom you have a **legitimate relationship** e.g. the patient you are caring for.
• ensure that office **doors and PCs are locked** when unattended.
• **raise concerns,** either through Datix or your line manager, if you become aware of an Information Governance incident or near miss.
• place **confidential waste** in confidentiality bins for shredding.
• Report any **unsolicited emails** (spam) to the IT Service Desk and delete them without opening them.
• **challenge** anyone you do not know who is in or entering a secure area.
• Use **post, secure encrypted emails and telephones** when discussing personal information. Fax machines are less secure and could lead to confidentiality breaches.

You SHOULD NOT
• hold confidential conversations in **public places** or discuss people you may inadvertently see e.g. sitting in the hospital café with anyone.
• save any confidential information to personal devices or to your **computer C-drive.**
• take patient hand overs, theatre list etc. **off site.**
• **share passwords** or smart cards .
• store confidential information on **unencrypted disks,** memory sticks, laptops and hard drives.

If in doubt please contact the Information Governance team for advice and guidance ruh-tr.IGQueries@nhs.net

Requests for information - Freedom of Information (FOI) requests

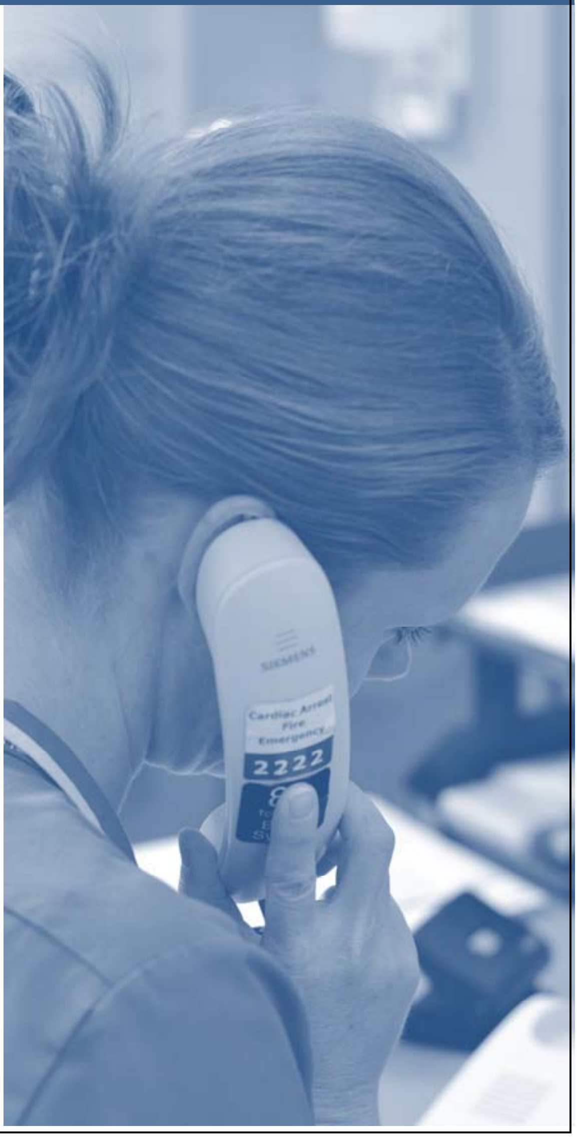
FIO requests would include general information such as emails and not confidential information such as staff personnel and patient records.

Should you receive an email from the FOI coordinator to provide information for an FOI request you are required to;

- Answer the request in the specified timeframe
- Complete the template provided.
- Notify the FOI coordinator should you not be the correct person to answer the request.
- Delegate the request to a relevant person should you be on annual leave, out of office etc.

Occasionally FOI requests are made to specific departments by members of the public. Should you receive an FOI then please forward to the FOI coordinator for them to complete the request.

There are exemptions which are listed in Appendix 2.



Requests for information - Subject Access Requests (SAR)

A SAR is a request from an individual to provide a copy of the information that an organisation holds **about them**.

This could be a patient, a member of staff or the public.

Should you receive a request for medical information then please forward the request to the medical records department. If you receive a request from a member of staff for their non-medical record then please contact the HR or IG team via ruh-tr.IGQueries@nhs.net.

Requests for information - responding to verbal requests from NHS bodies

If you receive a telephone request for patient information from a GP or other NHS body they can be verified by asking them security questions. Ask them to confirm:

- **The patient's Medical Records or NHS number and**
- **The patient's GP and**
- **The patient's full name.**

Requests for information - responding to verbal requests from PATIENTS

If you receive a telephone request for patient information from member of the public they can be verified by asking them to confirm:

- The patient's **full name** and
- The patient's **date of birth** and
- The patient's **address** and
- Their **relationship** to the patient

Ask yourself—do I have the consent of the patient to discuss their healthcare with another person?

If you receive a verbal request in person and you are not in a role that enables Millennium access to verify them then please refer the individual to a more appropriate member of staff.

Procedures that assure information security

Data Protection Impact Assessment (DPIA)

A DPIA is necessary where change impacts individual privacy or where personal/confidential information will be used in new ways.

The Trust's DPIA template can be used to assess the risks and to score the likely impacts of change.

Should you be implementing or changing a system or process then please seek IG guidance.

If you are undertaking a project to implement a new process, system or a change to an existing process/ system is planned it will be important to assess the need for a PIA.

Information Sharing Agreement (ISA)

Where it is proposed to share information with other organisations on an ongoing basis it is important to understand the purposes and the legal gateway under which this information will be shared.

Part of this process is writing a formal ISA, which the relevant organisations sign up to. This outlines the data to be shared, the method and purposes of sharing and details relating to information security.

Should you be seeking to share information with organisations on an ongoing basis then please seek the advice and guidance of the IG team.

Data Quality

Corporate Records Management (CRM)

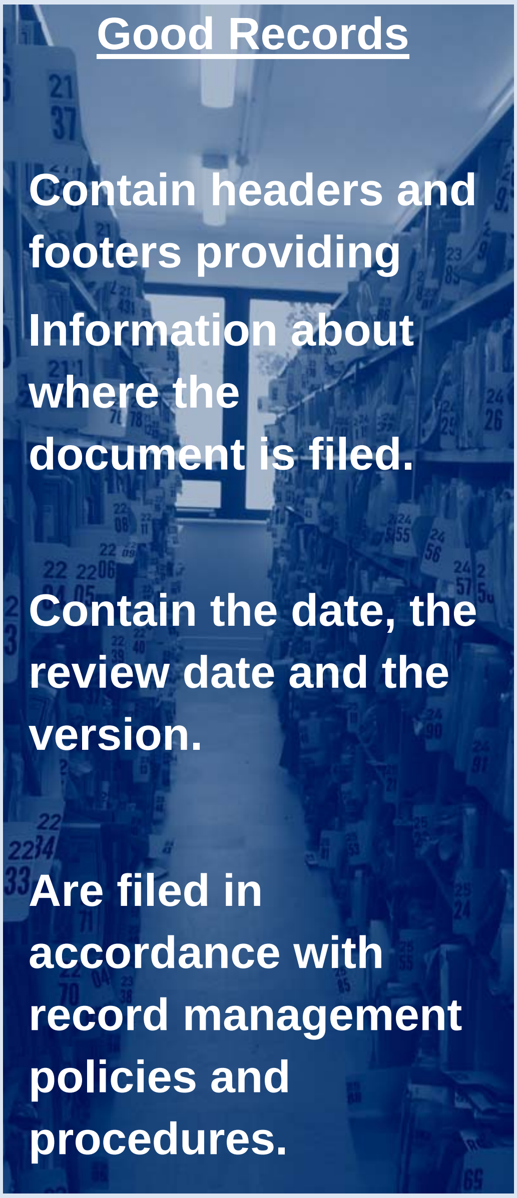
CRM concerns the way in which paper and electronic corporate records are stored and managed. Principally records must only be accessible by relevant people, all people who need access must know where records are kept and all documents must be version controlled.

Medical Records Management

There are some key principles to adhere to when documenting medical information within paper medical records, these can be found in the medical records policy for the Trust. Key considerations are that all information contained within a medical record is accurate and up-to-date, that records are kept securely and that only relevant individuals have access to records.

Good record keeping supports efficient and effective patient care, maximises income for the trust and provides an audit trail of actions and decisions.

Please note: medical records are owned by the Department of Health.



Good Records

Contain headers and footers providing Information about where the document is filed.

Contain the date, the review date and the version.

Are filed in accordance with record management policies and procedures.

Organisational Responsibilities

Datix Reporting & Manuals

Please report all incidents and near misses.

It is really important that Information Governance incidents and near misses are reported on Datix and/or to your line manager to report on Datix.

This is **not** to enable disciplinary action, this enables the IG team to **identify trends and risk areas.**

This means that processes can be changed and training can be amended in order to prevent further incidents.

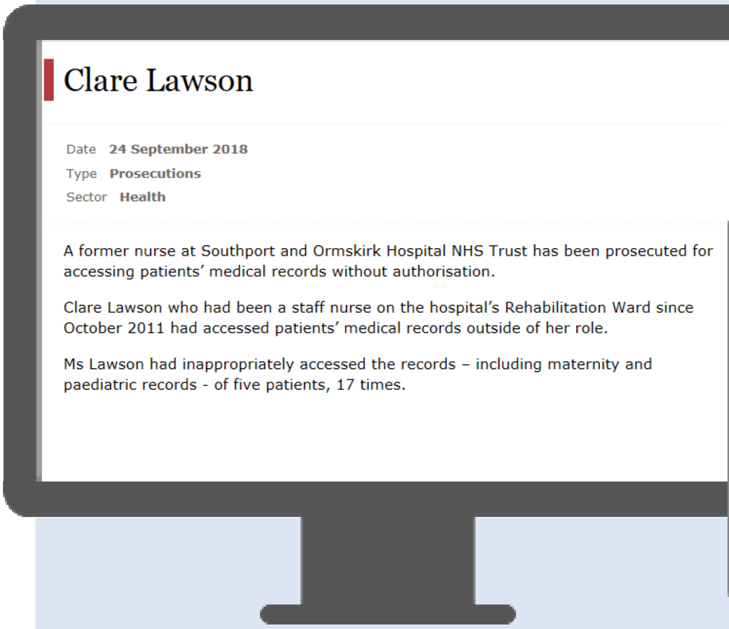
Information Governance Incidents

Recent incidents at the Trust

Incident	RUH response
Letter contains information about another patient	New rules implemented prohibiting copying and pasting into Millennium and limiting the number of records open at a time.
Safeguarding incident connected to family breakdown—an answerphone message gave an estranged parent information about a child.	Answerphone policy changed to prevent recurrence, including instructions for what messages can be left.

National Information Commissioners Officer (ICO) responses

The ICO oversees data protection in the UK. As the regulatory body the ICO has the powers to levy fines (between €10 million and €20 million) against organisations who have breached the Data Protection Act. The ICO also prosecutes individuals under the Data Protection Act and Computer Misuse Act as shown below which is an example of the first prison sentence.



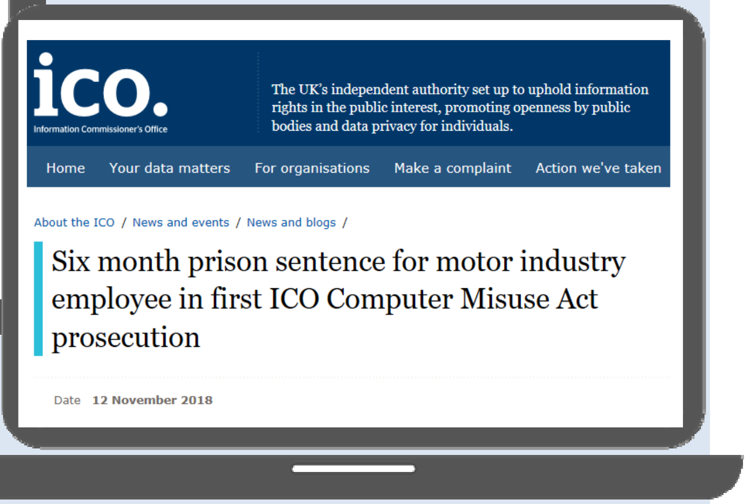
Clare Lawson

Date 24 September 2018
Type Prosecutions
Sector Health

A former nurse at Southport and Ormskirk Hospital NHS Trust has been prosecuted for accessing patients' medical records without authorisation.

Clare Lawson who had been a staff nurse on the hospital's Rehabilitation Ward since October 2011 had accessed patients' medical records outside of her role.

Ms Lawson had inappropriately accessed the records – including maternity and paediatric records - of five patients, 17 times.



ico. Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Home
Your data matters
For organisations
Make a complaint
Action we've taken
About the ICO / News and events / News and blogs /

Six month prison sentence for motor industry employee in first ICO Computer Misuse Act prosecution

Date 12 November 2018

Please note: You are responsible for **information security.**

Trust policies and contacts details

Further information

Email:

ruh-tr.IGQueries@nhs.net

IG pages:

http://webserver/staff_resources/governance/information_governance/index.asp

Policies pages:

http://webserver.ruh-bath.nhs.uk/staff_resources/governance/policies/az_of_policies.asp?menu_id=10

Trust Lead	Title	Contact details
Graeme Temblett-Willis	Head of Information Governance & Data Protection Officer	4416
Sue Cope	Information Governance Officer	6268
David McClay	Chief Information Officer	6250
Julie Clark	Freedom Of Information Coordinator	4309
Libby Walters	Senior Information Risk Owner	4032
Bernie Marden	Caldicott Guardian and Medical Director	4032

Appendix 1: Data Protection Act (DPA)

The DPA concerns any data that is identifiable, e.g. name, postcode, address, dates of birth, on line identifiers, physical, physiological, genetic, mental, economic, cultural or social identity about **living individuals.** We must comply with 6 principles of the act:

DPA Principles	
Processed lawfully, fairly and transparently	
1	**For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis' for processing, and there are six options which depend on your purpose and your relationship with the individual. There are also specific additional conditions for processing some especially sensitive types of data. For the purposes of direct care the lawful basis is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, and in respect of sensitive health data processing is necessary for the purposes of preventative or occupational medicine, the provision of health and social care or treatment or the management of health or social care systems and services.**
Collected for specified, explicit and legitimate purposes	
2	**This principle aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the patients and staff. There must be no surprises for the patients or staff as to what is happening with their data.**
Adequate, relevant and limited to what is necessary.	
3	**This principle relates to adequacy, relevancy and amount of data held. For example this means that while we would hold health information in a patient's record we would not hold their bank details. In clinical practice this means that if the police asked for information about a patient who had been assaulted the relevant episode of care would be disclosed but information relating to the patient's childhood medical conditions would not be.**
Accurate and kept up to date	
4	**This principle relates to data quality and accuracy. In practice this includes ensuring that patient information is correct and up-to-date and requires reception/administration staff to ask patients if their demographic details are correct at outpatient appointments. For clinical staff this would be ensuring that medical information is recorded accurately in the patient's medical record.**

Should not be kept longer than necessary

5

This principle relates to record retention. For example it would not be appropriate for us to hold patient records from 50 years ago relating to members of staff who are no longer employed here. Normally records will be destroyed when they have reached their full retention period and/or when they have been reviewed and deemed to no longer have any justified use. In practice this means following the Department of Health's retention schedule advice (please contact the IG department for more information).

Integrity and confidentiality. Security.

6

This principle relates to how information is processed and this must be in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This also means that when offices are unattended office doors should be secured, that staff do not share passwords or smartcards and that staff do not discuss patients in public places.

Accountability

Accountability makes you responsible for complying with the **GDPR** and says that you must be able to demonstrate your compliance. There are a number of measures that you can, and in some cases must, take including:

- **Maintaining documentation** correctly of your interaction with the patient and/or staff.
- Implementing **appropriate security** measures.
- **Recording and reporting** all personal data breaches via Datix.
- Taking a '**data protection by design and default' approach** and complete the necessary DPIA or ISA previously mentioned in this paper.

Personal data transfers

The **GDPR** restricts the transfer of personal data to countries outside of the EEA or international organisations.

These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out.

For assistance if this is a requirement you **must contact the IG Team.**

Appendix 2: Freedom of Information

Public Authorities (including NHS Trusts, local authorities, dentists, doctors, eye care services and pharmacists), are subject to the legal obligations of the Freedom of Information (FOI) Act 2000.

Public Authorities have only **20 working days** to respond to written information requests and we are not at liberty to ask why the information is requested.

This is the limit set out by law. Speak to the Head of Information Governance if you are unsure about the trusts procedures for dealing with FOI requests.

Some sensitive information might not be made available to members of the public. Trusts can turn down a freedom of information request if they think it will take longer than 18 hours to fulfill or if the data is commercially sensitive or if it is personally identifiable information e.g. information about 5 or less patients.