Information Governance, Confidentiality, Consent and Data Protection

Key Learning Points

- **What Information Governance is**

- **What YOU need to do to make this work**
  - ✓Follow the Caldicott Guidelines
  - ✓Provide a Confidential Service

- **Comply with the Law**
  - ✓Understand the Data Protection Act Principles
- **Follow HFR policies**

- **Keep Information Secure**

- **Input Quality Information**

What is Information Governance?

Describes the rules on handling information such as:

- Data Quality (making sure information is accurate and available),
- Records Management (a systematic method of recording information),
- Data Protection (which places obligations on how personal information is used) and confidentiality and security.

What do YOU need to do to make this work?

Information Governance is the responsibility of EVERYONE in HFR!

Data Protection Act 1998

UK law in the form of the Data Protection Act 1998 governs how organisations may use personal information (about living people), including how they acquire, store, share or dispose of it.

The Information Commissioners Office (ICO) is the UK's independent regulator set up to uphold the public's information rights by promoting data privacy for individuals (and openness by public bodies).

The ICO investigates complaints made by the public and provides guidance for the public and organisations.

Under the Act, organisations that process personal information must notify the ICO (unless they are exempt). The organisations' details are entered on a public register (available on the internet). Failure to notify is a criminal offence.

HFR is registered with the Information Commissioner
registration number: Z9579663

Data Protection Principles

It is your responsibility to understand the principles in relation to your role and the organisation.

Personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

8

4 Types of Information

1. Personal Information

•Information about an individual is personal information when it enables an individual to be identified. It is non-personal when it doesn't.

•This isn't always straightforward, e.g. a person's name and address are clearly personal information when presented together, but an unusual surname may itself enable someone to be identified. This is an important distinction in law.

2. Sensitive Personal Information

•Personal information is legally classed as sensitive when it makes reference to particular matters of an identifiable person, such as his/her health, ethnicity, religion, criminal record or sexual life. These are also listed in the Data Protection Act 1998.

•Other details, e.g. a person's bank account details, DNA or finger prints are not listed in the Data Protection Act 1998 but are still regarded as sensitive because of the damage and distress that could be caused if they were not properly protected.

•The rules set out in the Data Protection Act only apply to information about living individuals – not the deceased. This differs to the common law duty of confidentiality which continues after the death of the patient.

4 Types of Information

3. Confidential Information

•Personal and sensitive personal information is classed as confidential if it was provided in circumstances where an individual could reasonably expect that it would be held in confidence, e.g. a healthcare provider and patient.
•This applies to volunteers as well
•UK law says that health information is confidential
•Confidentiality is accepted to extend after the death of the patient or volunteer
•Whether information is confidential or not depends on the circumstances under which it was provided. If it is: private information about a person AND given to someone who has a duty of confidence AND expected to be used in confidence
THEN IT IS CONFIDENTIAL INFORMATION

4. Anonymous

• A reference number - if information is lost, it is unlikely that person can be identified.
•Think – could a patient with a rare illness be identified because of that?

7 Caldicott principles

INFORMATION to share or not to share

The Information Governance Review

7

The 7 Caldicott principles (2013) support the confidentiality and security controls on using patient information.

The principles should be used whenever a use of confidential information is being considered and in particular when there is an intention to transfer confidential information to another organisation:

1. Justify the purpose for using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum required.
4. Access should be on a strict need-to-know basis.
5. Everyone must understand their responsibilities.
6. Everyone must understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality

Your responsibility

- Personal data comprise name, address, phone number and date of birth.
- All members are responsible for ensuring that:
  - Any personal data which they hold, whether in Electronic or Paper format, is kept securely.
  - Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Volunteers should also be aware that regardless of any disciplinary action taken, they may also be liable to prosecution under Data Protection Act.
- Hester is the Information Governance and Data Protection Officer

Hart First Response

- HFR Home
- What We Do
- Who's Who?
- How To Join
- Event Cover
- Training Courses
- Photos
- Members Only
- Online Documents
- News
- CPR
- Lots of Links
- Affiliations
- Supporters
- Contact Us
- Donate Online

Registered Charity 1092333

HFR Members

Please join HFR on facebook

All new volunteers need to complete induction training, which is now possible online. First review and download the attached powerpoint HFR Induction slides, then complete the online quiz (you will need your volunteer ID to register).

Policies

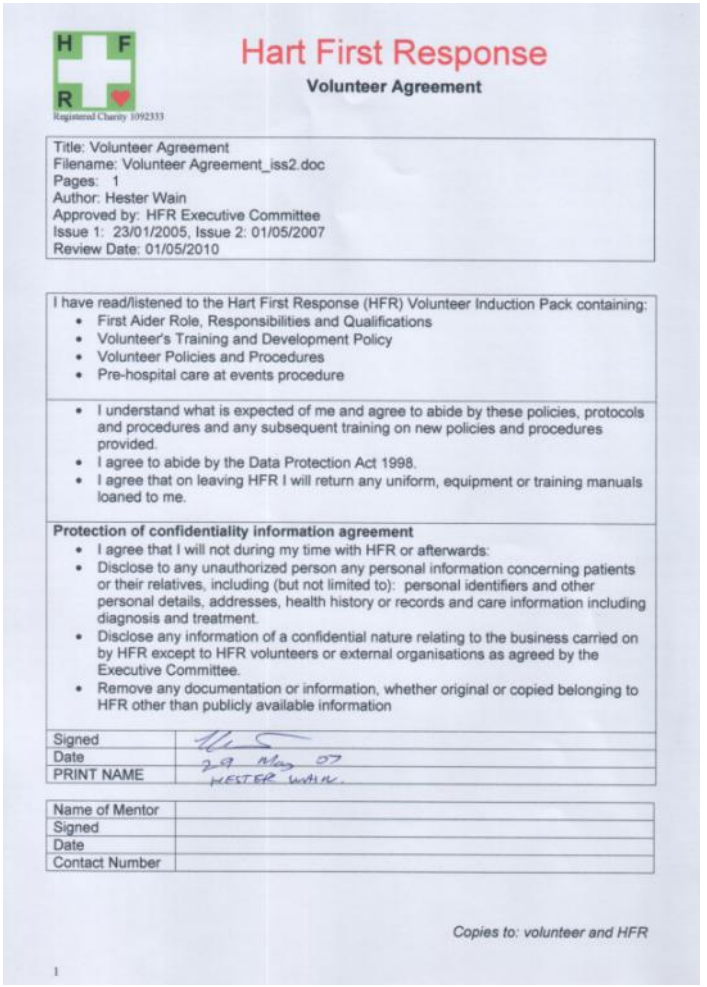
- Business Continuity Policy HFR Jan 2011.pdf
- Communication, Consent Being Open Policy HFR Mar 2011.pdf
- Compliments Concerns Comments and Complaints Policy HFR Jan 2011.pdf
- Driving Policy HFR Jan 2011.pdf
- Equality and diversity Policy HFR May 2011.pdf
- Healthcare records Policy HFR Mar 2011.pdf
- Infection prevention and control policy HFR Apr 2011.pdf
- Medical Devices Policy HFR Feb 2011.pdf
- Safeguarding policy HFR Mar 2011.pdf
- Safety and Suitability of Premises Policy HFR Jan 2011.pdf
- Scope of Practice Policy HFR Feb 2011.pdf
- Waste management Policy HFR Mar 2012.pdf
- Information Governance Confidentiality and Data Protection Policy HFR Mar 2012.pdf
- Risk Management and Incident Reporting policy HFR Mar 2012.pdf

HFR Volunteer Agreement

Protection of confidentiality information agreement

I agree that I will not during my time with HFR or afterwards:

- Disclose to any unauthorized person any personal information concerning patients or their relatives, including (but not limited to): personal identifiers and other personal details, addresses, health history or records and care information including diagnosis and treatment.
- Disclose any information of a confidential nature relating to the business carried on by HFR except to HFR volunteers or external organisations as agreed by the Executive Committee.
- Remove any documentation or information, whether original or copied belonging to HFR, other than publicly available information.



Hart First Response

Volunteer Agreement

Registered Charity 1092333

Title: Volunteer Agreement
Filename: Volunteer Agreement_iss2.doc
Pages: 1
Author: Hester Wain
Approved by: HFR Executive Committee
Issue 1: 23/01/2005, Issue 2: 01/05/2007
Review Date: 01/05/2010

I have read/listened to the Hart First Response (HFR) Volunteer Induction Pack containing:

- First Aider Role, Responsibilities and Qualifications
- Volunteer's Training and Development Policy
- Volunteer Policies and Procedures
- Pre-hospital care at events procedure

- I understand what is expected of me and agree to abide by these policies, protocols and procedures and any subsequent training on new policies and procedures provided.
- I agree to abide by the Data Protection Act 1998.
- I agree that on leaving HFR I will return any uniform, equipment or training manuals loaned to me.

Protection of confidentiality information agreement

- I agree that I will not during my time with HFR or afterwards:
- Disclose to any unauthorized person any personal information concerning patients or their relatives, including (but not limited to): personal identifiers and other personal details, addresses, health history or records and care information including diagnosis and treatment.
- Disclose any information of a confidential nature relating to the business carried on by HFR except to HFR volunteers or external organisations as agreed by the Executive Committee.
- Remove any documentation or information, whether original or copied belonging to HFR other than publicly available information

Signed	
Date	29 May 07
PRINT NAME	HESTER WAIN.

Name of Mentor	
Signed	
Date	
Contact Number	

Copies to: volunteer and HFR

1

Registered Charity 1092333

www.hartfirstresponse.org.uk

Do's and Don't's of Social Media

- Don't make disparaging remarks about HFR, its clients or fellow volunteers on a social network site
- Don't make any remarks on a social network site that may embarrass HFR organisation. In particular, do not air your grievances where countless others might be able to read all about it
- Don't identify patients in your care, or post information that may lead to the identification of a patient. If you do, you interfere with their privacy and breach the law on confidentiality
- Never post sexually explicit, racially offensive, homophobic or other unlawfully discriminatory remarks on your site

Patient Report Forms

- A healthcare record / patient report form (PRF) **must** be completed every time a patient is seen and examined, even if no treatment is given.
- The carbon copy is offered to the patient or given to the NHS ambulance crew
- Volunteers **must not** keep personal copies of patient details
- Volunteers **must not** attempt to contact any patient directly using information gained by completing the patient report forms

Input Quality Information

High quality means:

Complete

Accurate

Relevant

Accessible

Timely

Right information, Right place, Right time

•Accuracy is just one quality that we expect in records. But other qualities are also needed for the information to be useful, e.g. it would be pointless having information which was 100% accurate but wasn't available in time for it to be used.

•Information is used to make decisions throughout the health sector each day in all sorts of situations. Sometimes this information needs to be extremely high quality and complete, such as timely and accurate observations to help decide a patient's urgent condition and treatment.

Poor quality information

•Poor quality information is bad for patient care and bad for reputation, duplication causes confusion

•Incomplete data can lead to serious failures in service delivery

•Inadequate records (such as those completed in pencil) can lead to poorly planned care.

Handling Information

Holding it securely and confidentially

Obtaining it fairly and efficiently

Recording it accurately and reliably

Using it effectively and ethically

Sharing it appropriately and lawfully

Patient confidentiality

Patient Handover to Healthcare Professionals

- Ambulance NHS crew - give a verbal handover
- Give the carbon copy of the patient report form

Information requested by event organisers

- Do not provide full details of patients to the event organisers without the patient's consent.
- Patient report forms contain a "consent to datashare" section. You should ask the patient: "We may be asked to provide information on your injury/illness to the organisers along with your name and address etc, do you give you consent for us to associate your name with your injury/illness?". Patients do not have to give consent.
- The Officer In Charge (OIC) at an event will decide if details need to be passed on for health and safety reasons e.g. Motor Sport Association events or Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (1995)

Do not discuss the patient with anyone else (friends etc) at the event

Do not discuss anything with the press – refer them to the OIC

http://www.ico.gov.uk/

News releases - 2012

Belfast Trust fined £225,000 after leaving thousands of patient records in disused hospital
19 June 2012
Belfast Health and Social Care Trust has been served with a Civil Monetary Penalty of £225,000 following a serious breach of the Data Protection Act , the ICO said today.

ICO launches IT security guide for small businesses
18 June 2012
The ICO has today published a new guide for small and medium sized businesses, showing a series of clear, practical steps they can take to help make their IT systems safe and secure.

ICO statement in response to the publication of the Communications Data Bill
14 June 2012
The ICO has issued a statement in response to the publication of the Communications Data Bill.

Telford and Wrekin Council fined £90,000 following disclosure of vulnerable children's data
6 June 2012
Telford and Wrekin Council has been issued with a penalty of £90,000 by the ICO, following a breach of the Data Protection Act involving the disclosure of confidential and sensitive personal data relating to four vulnerable children.

NHS Trust fined £325,000 following data breach affecting thousands of patients and staff
1 June 2012
Brighton and Sussex University Hospitals NHS Trust has been served with a Civil Monetary Penalty of £325,000 following a serious breach of the Data Protection Act, the ICO said today.

ICO consults on new anonymisation code of practice
31 May 2012
The Information Commissioner's Office (ICO) has begun a public consultation on a new anonymisation code of practice. The code will provide guidance on how information can be successfully anonymised and how to assess the risks of identification.

London NHS Trust fined £90,000 for serious data breach
21 May 2012
Central London Community Healthcare NHS Trust has been fined £90,000 following a serious breach of the Data Protection Act, the ICO announced today.

ICO to revise publication scheme requirements
17 May 2012
The ICO has today announced that new changes will be made to the information public authorities will need to release proactively as part of their publication scheme.

ICO News June 2012

NHS Trust fined £325,000 following data breach affecting thousands of patients and staff

- Brighton and Sussex University Hospitals NHS Trust has been served with a Civil Monetary Penalty (CMP) of £325,000 following a serious breach of the Data Protection Act (DPA), the Information Commissioner's Office (ICO) said today.
- The fine is the highest issued by the ICO since it was granted the power to issue CMPs in April 2010.
- It follows the discovery of highly sensitive personal data belonging to tens of thousands of patients and staff – including some relating to HIV and Genito Urinary Medicine (GUM) patients - on hard drives sold on an Internet auction site in October and November 2010.
- The data included details of patients' medical conditions and treatment, disability living allowance forms and children's reports. It also included documents containing staff details including National Insurance numbers, home addresses, ward and hospital IDs, and information referring to criminal convictions and suspected offences.
- The data breach occurred when an individual engaged by the Trust's IT service provider, Sussex Health Informatics Service (HIS), was tasked to destroy approximately 1000 hard drives held in a room accessed by key code at Brighton General Hospital in September and October 2010. A data recovery company bought four hard drives from a seller on an Internet auction site in December 2010, who had purchased them from the individual.

ICO News January 2012

Health worker convicted of obtaining patient details unlawfully

•A former health worker has pleaded guilty to unlawfully obtaining patient information by accessing the medical records of five members of her ex-husband's family in order to obtain their new telephone numbers.

•Juliah Kechil, formerly known as Merritt, a former Health Care Assistant in the outpatients department at the Royal Liverpool University Hospital, was convicted under section 55 of the Data Protection Act at Liverpool City Magistrates Court today. She was fined £500 and also ordered to pay £1,000 towards prosecution costs and a £15 victim surcharge.

•Ms Kechil accessed the medical records of the five individuals between July and November 2009. Royal Liverpool University Hospital began an investigation in November 2009 when the defendant's father-in-law contacted the hospital after receiving nuisance calls which he suspected had been made by his former daughter-in-law. Having changed his phone number in July 2009 following unwanted calls from Ms Kechil, he was immediately concerned that there had been a breach of patient confidentially.

•Checks by the hospital revealed that all of the patients whose details had been compromised were not at any time under the medical care of Ms Kechil and she had no work-related reasons to access their records. She accessed the information for her own personal gain without the consent of her employer. The accesses were traced through audit trails which were linked to the defendant's smartcard ID.

ICO News December 2011

Receptionist unlawfully accessed sister-in-law's medical details

•A receptionist who unlawfully obtained her sister-in-law's medical records in order to find out about the medication she was taking has been found guilty of an offence under section 55 of the Data Protection Act.

•Usha Patwal, of Romford, was given a two year conditional discharge and ordered to pay £614 prosecution costs by Havering Magistrates Court today.

•The offence was uncovered when Patwal's sister-in-law received text messages indicating that the caller knew about the medication she was taking at the time. She then contacted her doctors' surgery - Gateway Medical Practice, Gravesend, Kent - to express her concerns. The investigation by the ICO uncovered that Ms Patwal had made a call to Gateway posing as an employee of the King George Hospital in Romford, Essex, on 29 December 2010. Further enquiries found that the sensitive medical information had been faxed to Ms Patwal at the Lawns Medical Centre where she was employed as a receptionist. The fax has never been found and Mrs Patwal did not co-operate with the ICO investigation by giving an explanation for her actions.

Unlawfully obtaining or accessing personal data is a criminal offence under section 55 of the Data Protection Act 1998. The offence is punishable by way of a financial penalty of up to £5,000 in a Magistrates Court or an unlimited fine in a Crown Court.

Disclosing information

Confidential information should not normally be used (which includes sharing and disclosing) unless one of the following criteria are met.

1. The person has given consent for the disclosure.
For patients:
• Consent may be implied for care purposes and related purposes that support or check the quality of care provided.
•For other purposes consent should be specifically sought.

2. There is a legal basis which permits or requires disclosure of confidential information.

3. There are exceptional circumstances (e.g. investigation or prevention of serious crime) where the overriding public interest outweighs the duty of confidentiality.

Information "required by statute"

Volunteers are required by statute to notify the relevant authority in the following cases. If possible the volunteer should refer the enquirer to the Officer in Charge of the event or the HFR Executive Committee:

- **s11, Public Health (Control of Disease) Act 1984** - Duty to notify proper officer of the local authority of the name, age, sex, and address of a person suffering from a notifiable disease or food poisoning;
- **s18, Prevention of Terrorism Act 1989** - Power to require the production of information from any person; also makes it an offence to fail to volunteer that information;
- **Regulations made under the Health and Safety at Work Act 1974**- Notification of industrial accidents and diseases;
- **s172, Road Traffic Act 1988** - Power to require any person to disclose information which may lead to the identification of a person guilty of certain offences.

Disclosure to Police

You are required to co-operate with the Police and must not break the law. You should not breach patient confidentiality (ie giving patient's name, address etc). However, in the following circumstances you are obliged:

- To inform the police of a motor vehicle collisions involving injury.
- To inform the police of an industrial accident (that needs to be reported via RIDDOR)
- To inform the police when a serious criminal event has occurred, such as assault or rape

You should not be providing any other details to the police and should not inform them of an overdose or illegal drug use by a patient. If any other information is requested, such as patient details or notes, please refer them to the OIC, who will refer them to the HFR Chair.

Disclosure

- When a patient does not consent to police or other agencies being called then their wishes must be respected and unless they are believed to be incapable of making an informed decision, or in extreme personal danger either from themselves or a third party, their right to confidentiality must be respected.
- When a patient has agreed to the police or other agencies being called then information may be given to those agencies that pertains to the crime and may assist them in their enquiries.

Security Breaches

Major causes of breaches include:

- Information disclosed in error
- Lost data/hardware
- Information lost in transit
- Stolen data or hardware
- A technical or procedural failure
- Breach arising from non-secure disposal

Confidential Waste

Includes:

- Patient records
- Volunteer records
- HFR Event Sheets
- Financial information that is considered sensitive
- Confidential contractual documents
- Exec. reports that are considered sensitive
- Any material containing personal information such as name, telephone number, address.

-> Dispose by shredding

Consent

No decision about me without me

- Valid Consent: The voluntary and continuing permission of the patient to be given a particular examination, treatment, operation or examination. Consent is only valid where it is given by an appropriately informed person who has the capacity to consent to the intervention in question
- Informed Consent: A patient's consent to a clinical procedure (or to participation in a research study) after being advised of all relevant facts and all risk involved.
- Capacity to Consent: The ability to receive, understand and retain information long enough to be able to make a decision. An individual must be assumed to have capacity unless it has been determined that they lack capacity.
- Duration of Consent: The length of approval gained by valid consent being given. This generally remains valid unless it is withdrawn by the patient, however, new information should be given to the patient as it arises, and consent regained.
- Duty of Care The absolute responsibility of a healthcare provider to treat and care for a patient with a reasonable degree of skill and care.
- Best Interests An act done or decision made under the Mental Capacity Act for or on behalf of a person who lacks capacity.

HFR Consent Statement

Before we examine or treat you, we need your consent. If you later change your mind, you're entitled to withdraw consent at any time.

- We will explain:
- How we intend to examine, or treat you.
- What the main treatment options are.
- What alternative treatments are available (*including no treatment*).
- What the intended benefits are.
- What risks (if any) may be associated with these treatments.
- Any extra procedures which may become necessary during the treatment.
- How you can expect to feel afterwards.

We will ask you:

- If you have any illnesses, or allergies which you may have, or have suffered from in the past.
- If you have any particular concerns.
- If there is any procedure you don't want to happen.
- If you consent to treatment.

Consent for young people

Aged 16–17

- People aged 16 or 17 are entitled to consent to their own medical treatment

Aged under 16 – the concept of "*Gillick* competence"

- Under 16 year olds who have sufficient understanding and intelligence to enable them to understand fully what is involved in a proposed intervention will also have the capacity to consent to that intervention. This is sometimes described as being "Gillick or Fraser competent"

Refusal of treatment

- The refusal of a competent person aged under 18 years may in certain circumstances be over-ridden by either a person with parental responsibility or the court.
- This power to over-rule must be exercised on the basis that the welfare of the young person is paramount.
- It may only be appropriate to over-rule a competent young person's refusal, if that person is at risk of suffering "grave and irreversible mental or physical harm".

Stored HFR Information

- Applicants' personal information (Electronic / paper)
- Back-up of all electronic HFR data/information
- CRB disclosures
- Email files
- Event Booking Forms containing organiser's personal details (Electronic / paper)
- Event Sheets - containing organiser and HFR volunteer's personal details (Electronic / paper)
- HFR database - contains HFR volunteer's personal details and names of paramedics, organisation/personal contact details
- Patient records (over 18 years old)
- Patient records (under 18 years old)
- Volunteers' personal information (Electronic / paper)

Acts etc

- Data Protection Act (1998)
- Access to Health Records Act (1990)
- Computer Misuse Act (1990)
- Electronic Communications Act (2000)
- Caldicott Principles (2013)
- The Human Rights Act (1998 Article 8)
- Common Law Duty of Confidentiality
- Data Protection Act 1998
- Freedom of Information Act 2000 (FOI)
- Environmental Information Regulations 2004
- Department of Health Records Management: NHS Code of Practice
- The Confidentiality Code of Practice
- Information Security Management BS7799

Acknowlegdements and References

County Durham and Darlington NHS
NHS Foundation Trust

- Information Commissioner's Office (ICO) http://www.ico.gov.uk/
- County Durham and Darlington NHS Foundation Trust www.cddft.nhs.uk/
- NHS Somerset Community Health