

General Protocol for Information Sharing

Signatories to the General Protocol

- Y Renfrewshire Council
- Y NHS Argyll and Clyde Board
- Y Renfrewshire and Inverclyde Primary Care NHS Trust
- Y Argyll and Clyde Acute Hospitals Trust

Purposes of information sharing

The protocol sets out the reasons these agencies agree to the sharing of personal information:

- Y Efficient and effective delivery of care services
- Y Improve quality of care / access to care
- Y Support national policy on joint working
- Y Support joint care planning and commissioning
- Y Support joint statutory reporting

Legislation and guidance

All partner agencies are subject to the same legislation governing the holding of personal information, the most significant being the **Data Protection Act 1998**. There are also professional codes of practice, policies (e.g. computer security, e-mail guidelines) and contractual conditions of employment applicable to individual agencies which add to the framework for information sharing. Particularly important here are the **Caldicott Principles** to which all NHS organisations are subject. The protocol document also makes reference to:

- Y Crime and Disorder Act 1998
- Y Human Rights Act 1998
- Y Common Law duty of confidentiality
- Y Freedom of Information (Scotland) Act 2002

A national model agreement was used as the basis for development of the Renfrewshire General Protocol document; this development was conducted by the multi-agency Single Shared Assessment Reference Group. The General Protocol will be augmented by specific protocols that deal with the arrangements and responsibilities for a particular information sharing purpose, e.g. Older Peoples Services. The operation of the protocol will be reviewed at appropriate intervals.

Key principles governing information sharing

- Y Multi-agency working creates an obligation for all partners to share information appropriately - in compliance with legislation and guidance.
- Y Non-NHS agencies recognise the Caldicott principles that apply within the NHS and will ensure requests for information are compatible with these principles.
- Y All parties acknowledge the fundamental duty of confidentiality of personal information and will not disclose information held by them without the explicit consent of the person concerned, unless there are statutory grounds /overriding justification for doing so.
- Y Information that is shared is used only in relation to specific purposes.
- Y All agencies have their own internal arrangements for conforming to Data Protection legislation (e.g. subject access request procedures) and other statutory duties.
- Y Individuals in contact with agencies will be fully informed about the information that is held about them.
- Y Relevant staff will receive specific guidance and training on the Adults with Incapacity Act.

- ÿ Individuals have the right to access Information that is provided by one agency to another, unless there are statutory grounds for requesting that a specific transfer is kept confidential from the subject.

Consent to disclosure of personal information

- ÿ All personal information is to be treated as confidential and ultimately owned by the subject - sensitive personal information should only be shared on the basis of the explicit, informed consent of the subject, unless there are statutory grounds and/or overriding justification for not observing this constraint.
- ÿ Seek at the earliest opportunity when the need for information sharing is identified.
- ÿ Ensure consent is given on an informed basis and is recorded formally using the common consent form. Consent is only gained legitimately where the subject is made fully aware of the purposes of information sharing.
- ÿ Information is to be shared and used only in relation to the specific purposes for which consent was given - i.e. consent will be treated as limited in scope and time applicable.
- ÿ Explain right to withhold consent., but advise of consequences for service delivery and support for personal needs.
- ÿ The Adults with Incapacity (Scotland) Act 2000 makes provision for either a guardian or, if there is none, a public authority, to act on behalf of individuals who are not able to represent themselves. Every attempt must be made to explain such procedure to the client and any guardian must be treated as having the same right as the data subject.
- ÿ Actual disclosure of sensitive information must be preceded by a check for a record of consent. Even where consent exists, disclosure of sensitive information should only take place where it is critical to the case.
- ÿ Disclosure of sensitive information without consent may be deemed necessary for, but this should only be undertaken after consultation with a person or persons appointed by the agency to advise or rule on such matters (e.g. Legal Services).

Transfer and use of personal information

The protocol gives clear guidance on the standards that should be applied when actually transferring personal information, to ensure the security and confidentiality of the information. The specifics of this are covered in summary of the Care of the Elderly protocol, but important general provisions are:

- ÿ There must be clear, unambiguous identification of the subject.
- ÿ The content of information transferred should make clear the distinction between fact and opinion.
- ÿ If it appears necessary to use personal information for a purpose other than that originally identified, then a formal process of seeking further consent from the data owner should be undertaken. The owner then has the responsibility to obtain consent from the person or take the decision that circumstances warrant the further use taking place without consent.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

More information on Data Protection guidance and a range of relevant links can be found at:

[Http://www.dataprotection.gov.uk/dpr/dpdoc.nsf](http://www.dataprotection.gov.uk/dpr/dpdoc.nsf)

Caldicott Principles

These principles govern the processing of personal information within NHS agencies.

Mnemonic (Fiona Caldicott)

Formal justification of purpose
Information transferred only when absolutely necessary
Only the minimum required
Need to know access controls
All to understand their responsibilities
Comply with and understand the law.

Explanation

Justify the purpose(s)

- ÿ Every proposed use or transfer of patient-identifiable information within or from the organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Do not use patient-identifiable information unless it is absolutely necessary

- ÿ Patient-identifiable information items should not be used unless there is no alternative.

Use the minimum necessary patient-identifiable information

- ÿ Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Access to patient-identifiable information should be on a strict need to know basis

- ÿ Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

Everyone should be aware of their responsibilities

- ÿ Those handling patient-identifiable information - both clinical and non-clinical staff - must be aware of their responsibilities and obligations to respect patient confidentiality.

Understand and comply with the law

- ÿ Every use of patient-identifiable information must be lawful.

Consent issues and terms

INFORMED CONSENT - Mrs Macdonald was discharged from hospital after a hip replacement and she is now talking to the OT about aids to help her bathe herself. She understands when the OT explains about consent, and states that she is perfectly agreeable for information about her mobility difficulties to be given to the other services that might be able to help her cope with the situation.

EXPLICIT CONSENT – Mrs Macdonald signs the form that the OT offers her.

IMPLIED CONSENT – No form was signed, nor was any conversation (about consent to share information about her) held with Mrs Macdonald, but her parting words to the OT are “Mind you get that District Nurse out here soon, now, and someone to run to Tesco for me would be a real help too”. From this, it is taken that Mrs M means it is all right to pass on information about her to the other services.

IMPUTED CONSENT – The OT and Mrs Macdonald did not actually discuss this aspect, but Mrs M looks after a profoundly deaf grandson while the child’s parent is at work, and on previous occasions she has been happy to share information about herself with the child’s team. So now, the OT thinks it is likely she would consent to information about her current difficulties being shared with another team also.

ASSUMED CONSENT – Mrs Macdonald is too “excited” to settle down and talk about what happens next, and the OT cannot get her to concentrate on what consent means. She decides that Mrs M *would* have agreed if she had actually had the conversation, and continues as if Mrs M *had* done so.

PERMISSIBLE BREACH OF CONFIDENTIALITY –Where there is a notifiable disease, or a likelihood the client may be violent, for example, or perhaps there is a child protection issue, it is permitted to share information about the client even if their consent is not given, but the risk must be so great that it means the breach of privacy is “proportionate” – that is, it matches the circumstances.

THE FAIR AND LAWFUL USE OF CLIENT-RELATED INFORMATION – This phrase, taken from the Data Protection Act of 1998, would be used by a court to decide if a **BREACH OF CONFIDENTIALITY** (see above) were right or wrong. The court would decide on the basis, generally speaking, of whether the breach of privacy meant the public’s trust and confidence would be less as a result.

DATA PROCESSING – Return to “Mrs Macdonald” and point out that every step of her care, would involve collecting, using and sharing data. All of this would be data processing, not merely elements on a computer

Definition of sensitive personal information

The Data Protection Act defines eight categories of sensitive personal data. These are:

- A) the racial or ethnic origin of data subjects;
- B) their political opinions,
- C) their religious beliefs or other beliefs of a similar nature,
- D) whether they are a member of a trade union,
- E) their physical or mental health or condition,
- F) their sexual life,
- G) the commission or alleged commission by them of any offence, or
- H) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.