

Children's Centre Information Sharing Protocol

Children's Centre Information Sharing Protocol

Contents

- 1 Purpose
 - 2 Introduction to Children's Centres
 - 3 Introduction to information sharing
 - 4 Information sharing principles
 - 5 Documentation
 - 6 Security
 - 7 Review
 - 8 Partner Agencies
 - 9 Signatories
-
- Appendix 1 Legislation and guidance
 - Appendix 2 Data Protection Act – staff instructions
 - Appendix 3 Children's Centre registration form
 - Appendix 4 Guidance on terms used in the protocol

Children's Centre Partnership Information Sharing Protocol

1 Purpose

The Caldicott Requirements state that an agreed, signed protocol must be in place to facilitate the sharing of patient information between agencies. The purpose of this protocol is to cover the principles governing the roles and responsibilities of partners with regard to information sharing between the Children's Centre and its partner agencies in order to fulfil Children's Centre objectives.

2 Introduction to Children's Centres

Children's Centres are part of the local system of universal children's services, providing easy access to a range of community health services, parenting and family support, integrated early education and childcare, and links to training and employment opportunities for families with children under the age of five. Children's centres are a key mechanism for improving outcomes for young children while reducing inequalities between the poorest children and their peers, as well as helping bring an end to child poverty.

The Apprenticeships, Skills, Children and Learning Act 2009 now defines Children's Centres in law. It places duties on local authorities in relation to establishing and running children's centres. It also places duties on Primary Care Trusts and Jobcentre Plus to consider regularly whether the early childhood services they provide should be delivered through children's centres in the area. This links with their duties as partners within the Children's Trust Board to plan and review the Children and Young People's Plan

3 Introduction to Information Sharing

Inadequate information sharing can have serious consequences. All Children's Centre partnership agencies are committed to sharing information in the interests of the well-being of children and families and for the purposes of providing effective joined up services to them and ensuring that children reach their potential.

4 Information sharing principles

4.1 This protocol covers information sharing in the context of collaborative work between the Children's Centre and its partners. The protocol relies on the existing and developing legislation and guidance that relate to safe and secure information handling (see Appendix 1).

- 4.2 Each partner agency will be responsible for ownership of the information within their own organisation and will implement their own internal confidentiality and security policies and systems.
- 4.3 It is the responsibility of every agency to this agreement to ensure that they are registered under the Data Protection Act 1998. This process is called 'Notification'.
- 4.4 Each partner agency is responsible for the issue of specific guidance and training for staff, to ensure compliance with their statutory responsibilities and with this protocol. (Appendix 2 shows instructions which could be issued to staff to outline their responsibilities under the Data Protection Act 1998). Any breaches of confidentiality by staff will be dealt with according to the policies and procedures of their employing organisation.
- 4.5 The Children's Centre Registration Form (see Appendix 3) is used to obtain consent from families to share information. It is the responsibility of partner agencies to ensure that staff are trained to provide sufficient information for parents to understand why information is needed, what is likely to be done with it and whom it may be shared with, at the time of registration.
- 4.6 Once signed, the Registration Form will provide evidence of consent for information sharing between all partner organisations. A copy of the Form must go to the Children's Centre core team to be recorded on the eStart database.
- 4.7 Information will be shared on a 'need to know' basis with a view to fulfilling Every Child Matters objectives. Operational Managers will adjudicate in any 'grey areas' and the final decision will be recorded.
- 4.8 Requests for information from another agency should be in writing and include: date of the request, name and other identifying information of the individual about whom the information is requested, purpose for which the information is required, and name and designation of the person requesting the information. In every case, the disclosure should not be sought unless it supports the purpose of this protocol.
- 4.9 Information will not be shared with partner agencies without consent, unless there is a legal requirement to do so e.g. to

comply with Child Protection requirements. When information is disclosed to a partner agency, the Children's Centre will retain ownership of it and the agency must undertake not to disclose it to a third party without consent. A record of the disclosure will be kept in the partner agency's client notes.

- 4.10 In some situations, disclosure in the public interest may override the duty to maintain confidentiality. In this context 'in the public interest' will be taken to mean there are reasonable grounds to believe that serious harm will occur if information is not disclosed. In these circumstances, a clear record detailing the reasons for the requested disclosure, outlining the decision-making process and explaining the reasons for the final decision will be kept.
- 4.11 Although the Data Protection Act places no restriction on the disclosure of information that does not identify individuals, precautions will be taken to ensure that such information is truly anonymised.

5 Documentation

- 5.1 Documentary information should only be kept for the minimum period necessary, after which the information should be returned to the originator or destroyed.
- 5.2 Disclosures and requests for disclosures must be recorded and retained by each agency. Decisions on disclosures reached at meetings must be minuted.

6 Security

Each agency will take appropriate measures to ensure that security arrangements are in place to prevent unauthorised access to, and disclosure of, personal information and will be open to scrutiny by other parties to this protocol upon request.

Each agency will nominate a designated person who will assume responsibility for the operation of this protocol and for the requesting and disclosure of information, security and confidentiality.

Appendix 1

1.1 Legislation and guidance

The main legislation governing individuals' rights and relating to security and confidentiality that must be considered are:

Human Rights Act 1998	Article 8 – a right to respect for private and family life, with exception of public interest. Article 3 – prohibition of torture or degrading treatment or punishment
Freedom of Information Act 2000	Individuals right of access to information held by public authorities
Regulation of Investigatory Powers Act 2000	Allows organisations to monitor automated communications e.g., email
Data Protection Act 1998	Sets out 8 key principles for sharing information. Individual's rights to confidentiality and security for their information and their right to access their own records.
Crime and Disorder Act 1998	Duty on all to prevent offending by children and young people; provides basic legal authority to disclose personal information where necessary to implement the act; promotes greater involvement of victims
Computer Misuse Act 1990	Makes it an offence for any user to gain unauthorised access to information on a computer
Children's Act 1989 and 2004	Provides the legal underpinning for the transformation of children's services as set out in the Every Child Matters: Change for Children programme
Childcare Act 2006	Formalise the important strategic role LAs play in improving the five ECM outcomes for all pre-school children & reduce inequalities in these outcomes, secure sufficient childcare for working parents and provide a better parental information service.

The Apprenticeships, Skills, Children and Learning Act 2009	The Act gives children's centres a specific statutory basis, and places new duties on LAs to establish and maintain sufficient numbers to meet local needs
Caldicott Guidance	Recommends good practice principles to be used to safeguard NHS patient confidentiality. Requires an information sharing protocol
NHS and Community Care Act 1990	
NHS Services and Children's Centres- how to share information appropriately with children's centre staff	A leaflet for all staff working in, from, and with, Sure Start Children's Centres and explains how sharing needs to be done in an appropriate way, in accordance with the law.
Mental Health Act 1983	
Carers (Recognition and Service) Act	
Together for Children Toolkit: Health Information & Data Sharing for Children's Centres	A collection of resources and materials set in the context of the guidance NHS Services and Children's Centres- how to share information appropriately with children's centre staff
The Adoption Act 1976	
The Health Act 1999	
The Health and Social Care Act 2001	

1.2 Details of Legislation and Guidance Summary

1.2.1 The Human Rights Act 1998

This Act became law on 2 October 1998. It binds public authorities, including Health Authorities, Trusts, Primary Care Groups and Social Care and Health agencies, to respect and protect an individual's human rights. This will include an individual's right to privacy

(under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

1.2.2 Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information.

1.2.3 The Access to Health Records 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons' records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

1.2.4 The Data Protection Act 1998

The Data Protection Act 1998 covers manual as well as computerised information and sets the rules for processing (including obtaining, altering, disclosing or destroying) personal information. It requires anyone processing personal information about a living individual to tell him/her how it may be used, who it may share with and on what

basis. It also gives that individual the right to see that information, subject to certain conditions, the right to require inaccurate information to be amended or deleted and under some circumstances the right to prevent processing.

The following are the eight Data Protection Principles, which Sure Start Agencies seek to uphold:

- 1 Obtain and process personal data fairly and lawfully.
- 2 Process personal data only for the purpose, listed in each Partner Agency's Registry entry.
- 3 Only hold personal data, which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
- 4 Ensure personal data is accurate and, where necessary, keep up to date.
- 5 Hold personal data for no longer than is necessary.
- 6 Allow individuals access to information held about them and, where appropriate, correct it or erase it.
- 7 Take security measures to prevent unauthorised or accidental access to, alteration, disclosure, loss or destruction of personal data.
- 8 Only transfer the data to other countries that have suitable data protection controls in place.

1.2.5 Caldicott Guidance

The Caldicott Committee, chaired by Dame Fiona Caldicott reviewed the way patient information is used and handled in the NHS. The Committee recommended all NHS organisations should appoint a Caldicott Guardian responsible for safeguarding the confidentiality of patient information. It also recommended good practice principles to be used to safeguard patient confidentiality. In summary, these principles are:

- a) Justify the purpose(s) of every proposed use or disclosure of information
- b) Do not use patient-identifiable information unless it is absolutely necessary
- c) Use the minimum necessary patient-identifiable information
- d) Access to patient-identifiable information should be on a strict need-to-know basis. Everyone with access to

patient-identifiable information should be aware of their responsibilities

- e) Understand and comply with the law

1.2.6 Kent Safeguarding children's board (KSCB)

All agencies have a professional responsibility to safeguard children and where child protection concerns exist to work in accordance with the KSCB Safeguarding Children Procedures

1.3 Relevant Health and Social Services Circulars

HSC2000/009	Data Protection Act 1998: protection and use of patient information
HSC1998/203	Health records requests for access by patients and their representatives
HSG(96)18	The protection and use of patient information
LASSL2000-2	Data Protection Act 1998: guidance
LASSL(98)16	Data Protection Act 1998 draft guidance
LASSL(96)5	The protection and use of patient information
MISC(97)52	Faxing of safe haven amendments go live
HSC1999/053	For the Record (Preservation, retention & destruction of records under the Public Records Act 1958) and records management strategy
HSC1998/217	Preservation, retention and destruction of GP general medical services records relating to patients
HSG(91)6	Access to Health Records Act – A guide for the NHS
IMGF5498	A guide to implementing an awareness programme (The Information Security Resource pack)
HSG(96)15	The NHS IM&T Security Manual
HSG(96)18	The Protection & Use of Patient Information

Appendix 2

DATA PROTECTION ACT – STAFF INSTRUCTIONS

The Data Protection Act became law in November 1985, and has subsequently been amended by the 1998 Act, and requires that any personal data, i.e., data from which a living person can be identified, which is held on a computer or in paper form, is kept securely and managed properly. The people or organisations that process that personal data (Data Controllers) must be registered with the Information Commissioner's Office. This registration process is called Notification under the legislation. The registration details include all persons or bodies from whom the data may be collected and more importantly to who it may be disclosed. The act also gives rights to the people the information is about i.e. the right of subject access, lets individuals find out what information is held about them on payment of a fee.

In addition, the Act imposes certain conditions on the users of data. Broadly these are:

1. The data must be obtained and processed fairly and lawfully.
2. The data shall only be processed for specified and lawful purposes.
3. The data must be adequate, relevant and not excessive for the purpose for which it is held.
4. The data shall be accurate and where necessary, kept up to date.
5. The data shall not be kept longer than is necessary for the purpose for which it is held.
6. An individual who is the subject of the data shall be entitled to be informed whether any data is held about them, to have access to that data corrected or erased where appropriate.
7. Appropriate security measures must be taken to prevent loss, destruction, alteration and unauthorised access or disclosure of personal data.
8. The data should only be transferred to other countries that have suitable data protection controls.

It is therefore vitally important that the following procedures are adhered to:

1. No data is disclosed to a third party without authorisation from the Data Monitoring Officer in liaison with the relevant Core Team member.

2. That data is safeguarded against unauthorised access. For example, do not leave a terminal unattended whilst it is still logged into a system.
3. Computer print outs should be kept in a secure place when not being used. Any printout containing personal data should be shredded when no longer required.
4. That any proposed changes in the use of data must be reported in writing to the Data Monitoring Officer.
5. That any proposed new systems for Microcomputers or word processing equipment must be notified in writing to the Data Protection Officer, in order that the appropriate registration can be made.

Remember – these instructions are designed to help you. If you ignore them, it will be YOU that could be prosecuted under the Act.

Appendix 3

Registration form for Children's centres

Please see the following link:

http://www.clusterweb.org.uk/chc/chc_documents_estart.cfm

Appendix 4

Guidance on Terms Used in the Protocol

Anonymised

Data from which an individual cannot be identified by the recipient of the information. The name, address and full postcode must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the patient. NHS numbers or other unique numbers may be included only if recipients of the data do not have access to the 'key' to trace the identity of the patient using this number. Taken from the GMC guidance on "Confidentiality, Protecting and Providing Information".

Consent

Consent implies both choice and understanding. "Consent" given under duress or coercion is not, in fact consent. "Consent" given without a reasonable understanding of the purposes for which information is to be processed and of the type and purposes of disclosures envisaged is equally invalid.

Taken from the Information Commissioner' draft guidance "Use and disclosure of medical data" (May 2002).

Consent	Agreement, either express or implied, to an action based on knowledge of what the action involves, its likely consequences and the option of saying no. (GMC)
Express Consent	Consent which is expressed orally or in writing except where service users (patients) cannot write or speak, when other forms of communications may be sufficient. (GMC)
Implied Consent	Consent which is inferred from a person's conduct in the light of facts and matters which they are aware of, including the option of saying no.

Taken from the 'Draft' Cambridge Information document 'Confidentiality Guidance – Consent to Disclose Personal Information'.

Confidentiality

The common law **duty of confidentiality** requires that unless there is a statutory requirement data should only be used for purposes that the subject has been *informed about* and has *consented* to. It is important to remember that information is provided in confidence when it *appears reasonable to assume* that the provider of the information believed that this would be the case.

Personal data which is subject to an obligation of confidentiality has a number of characteristics:

- ◆ The information is not in the public domain or readily available from another source;
- ◆ The information is of a certain degree of sensitivity, such as medical data;
- ◆ The information has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a customer and a bank or a patient and doctor.

The courts have generally recognised three exceptions to the duty of confidence:

- ◆ When there is a legal compulsion (for instance a statutory requirement or a court order);
- ◆ Where there is an overriding duty to the public;
- ◆ Where the individual to whom the information relates has consented.

Privacy and Confidentiality

A breach of confidentiality is almost certain to involve a breach of privacy. However, a breach of privacy does not necessarily entail a breach of confidentiality. There will be a breach of privacy if, for instance, patient records are stolen from a GP's surgery. There will not, however, be a breach of confidentiality if it had not been the GP's intention to disclose the records to a third party. (Depending upon the security with which the records were kept there may be issues of negligence or a failure to satisfy a duty of care.) The

issues of confidentiality and privacy are thus related, but by no means identical. However, measures taken to enhance privacy (whether in the field of IT security or the vetting of staff) will generally be supportive of the duty of confidence.

Taken from the Information Commissioner' draft guidance "Use and disclosure of medical data" (May 2002).

Document Properties			
This Policy has been written by:		Researcher for Early Years & Childcare and Access to Information Co-ordinator with support from the Children's Centre Monitoring Group	
Title		Children's Centre Information Sharing Protocol	
Version History			
April 2008	v1		First release- final version
March 2010	v2.1		Second release – updated version released for consultation
April 2010	v2.2		Second release- final updated version