

All correspondence to:

The Breastfeeding Network
PO Box 11126, Paisley PA2 8YB
Tel: 0844 412 0995
e-mail: admin@breastfeedingnetwork.org.uk
www.breastfeedingnetwork.org.uk

The Breastfeeding Network

Information Governance Policy

Issue Date: October 2010
Updated: 20 December 2010

Review Date: October 2012

To find your nearest Breastfeeding Supporter call the **Supporterline 0300 100 0210**

Calls to 0300 numbers cost no more than calls to UK numbers starting 01 and 02 and will be part of any inclusive minutes that apply to your provider and call package

The Breastfeeding Network is a Company Limited by Guarantee Registered in Scotland Company No. 330639
Registered office Alexander Sloan, Chartered Accountants, 38 Cadogan Street, Glasgow, G2 7HF
The Breastfeeding Network is a Registered Scottish Charity No SC027007

BREASTFEEDING NETWORK INFORMATION GOVERNANCE POLICY

CONTENTS

1. Introduction
2. Definition of Information Governance
3. Scope of the Document
4. Policy statement
5. Aim of this Strategy
6. Information Governance Management
7. Defining the different types of information and its Storage
8. Confidentiality and Data Protection Assurance
9. Information compliance (including Data Protection)
10. Information Security Assurance
11. Records Management
12. Information Sharing
13. Information Governance– annual assessment of compliance

Annex

Annex 1: Individuals with specific duties for Information Governance.

Annex 2: Six Caldicott Information Management Principles

Annex 3: The Data Protection Act and Principles

Annex 4: Breastfeeding Network – our guarantee about client records

Annex 5: Records Retention Summary

1. Introduction

The Information Governance Strategy and the resulting policy for the Breastfeeding Network is based upon national best practice models set out in the NHS Information Governance Toolkit. The policy sets out information handling standards and describes the tools BfN will use to achieve these standards to develop a consistent approach to handling personal and organisational information.

2. Definition of Information Governance

Information Governance is a framework to bring together all of the requirements and best practice standards that apply to the handling of information. This is wide ranging and can be about volunteers, employees and service users. It is particularly concerned with personal and sensitive information, but it also incorporates information about the organisation, ensuring that information is accurate and handled in a confidential and secure manner to appropriate ethical and quality standards in order to deliver the best possible service.

3. Scope of the Document

The scope of this strategy covers the management of information handling activities and measures compliance against a number of key interlinking standards covering the following strands:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information compliance (including Data Protection)
- Information Security Assurance
- Information Quality Assurance
- Records management
- Information sharing

The NHS Operating Framework 2009/2010 and supplementary guidance provided in Informatics Planning 2009/10 require that BfN as a provider of services to the NHS should work within the NHS Information Governance Assurance Framework and demonstrate compliance with all key information governance requirements. These key requirements are contained within the Information Governance Toolkit, an online assessment tool, which enables organisations to evidence compliance.

4. Policy statement

The policy sets out information handling standards and describes the tools BfN will use to achieve these standards to develop a consistent approach to handling personal and

organisational information. This will lead to improvements in information handling activities and improve service user confidence in the Breastfeeding Network.

5. Aim of this Strategy

- To promote the effective and appropriate use and sharing of information.
- To enable understanding of our performance and manage improvements in a systematic and effective way to meet the Information Governance Assurance requirements set out by the Chief Executive of the NHS.
- To encourage joint working between the Breastfeeding Network and the NHS, preventing duplication of effort and enabling more efficient use of resources.

Objectives

- To ensure that personal data on service users, volunteers and employees is handled securely and legally by all BfN volunteers and employees.
- To provide a framework to bring together all the requirements, standards and best practice that apply to the handling of personal information.
- To establish guidelines to ensure information is accurately recorded and to ensure it is accessible when needed.
- To monitor progress against agreed standards and plan improvements.

6. Defining Different Types of Information and its Storage

Information stored by the Breastfeeding Network must be:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

Information can be classified in a number of different ways. Information about individuals is considered **personal** when it enables an individual to be identified, or **non-personal** when it doesn't.

Personal information - for example contact record sheets or trainee / staff records, may

be held subject to obligations of confidentiality and may be legally sensitive as defined by the Data Protection Act 1998.

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, this applies both to service users, learners, volunteers and employees. Confidentiality is generally accepted to extend after death. Personal information may be classed as legally sensitive when it makes reference to particular matters, such as health, ethnicity or sexual life, which are listed in the Data Protection Act. [See section 8, annex 3 and link on p16 for further information]

“Person identifiable information” relates to information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. “Sensitive information” can be broadly defined as that which if lost, misdirected or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, data defined as sensitive under the Data Protection Act 1998, for example, financial and security information about an organisation is likely to be deemed “sensitive”, as are an individual’s bank account details.

Person based but anonymised information - for example, Call record sheets or BfN Breastfeeding Centre monthly record sheets, are not subject to the same restrictions and requirements as personal information as no-one can be harmed or distressed by its disclosure. Neither Confidentiality Law nor the Data Protection Act applies to person based information that has been effectively anonymised. This means that taking steps to anonymise information is often very important as it enables information to be processed without having to satisfy strict legal requirements.

Documents - that are not about individuals, for example BfN accounts are not considered personal information but may be classed as confidential. This could be, for example, for commercial reasons or because they contain legal advice.

They may also be regarded as sensitive in a general sense because of their subject matter.

7. Confidentiality and Data Protection Assurance

BfN has appointed Mary Broadfoot as the Caldicott/IG Lead. Together with the BfN Policy Implementation Team they have responsibility for advising on confidentiality and other Information Governance issues. The role of the Caldicott/IG Lead is to ensure that all members of the Breastfeeding Network understand the Information Governance rules that apply to them and that there are documented policies and procedures for everyone to follow. The Caldicott/IG Lead is responsible for developing, implementing and monitoring Information Governance procedures and working practices and for providing advice when requested. BUT it is the responsibility of everyone in BfN to comply with the procedures and working practices so we are all equally responsible for making sure information is kept safely.

There are **Six Caldicott Information Management Principles** that provide guidance when handling client information. These are questions that you should ask yourself before processing or disclosing personal information

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

Additional information to help us maintain a confidential service is available from the 'Confidentiality: NHS Code of Practice'; (this link can be found in the summary section of this document). This requires BfN to look at ways to improve the confidentiality of the service we offer – to find better ways to protect, inform, and provide choice for service users. This will include training for relevant people within the organisation and the development of systems to enable possible breaches or risk of breaches to be identified and rectified with confidentiality audits to discover whether any possible breaches occurred through deliberate misuse of systems, or of poor controls. Confidentiality audits include both electronic records management systems and paper record systems.

[See annex 3 and link on p16 for further information]

8. Information compliance

Data Protection

The Data Protection Act 1998 applies to all organisations in the UK which process personal information. We can face legal action if any of the eight Data Protection Principles of the Act has been breached.

The 8 Data Protection Principles - Personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept 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

We must have the consent of mothers before we process any information about her. Explicit consent means clear, voluntary, freely given indication of preference or choice, where the available options and consequences have been made clear. Consent can be given orally or in writing.

Individuals generally have the right to see the personal information held by an organisation. Applications or 'Subject access requests' must be in writing with enough information for the organisation to identify the records. BfN must comply with the request within 40 days of receipt, but wherever possible information should be provided within 21 days.

[See annex 3 and link on p16 for further information]

9. Information Security Assurance

This section covers both manual and electronic records to safeguard person identifiable information from being disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated within and outside of BfN. BfN will maintain an information asset register for its information, software, hardware, and services which includes the owner and location of each asset and audit all equipment, static & portable. Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

Risk assessments will be carried out to identify potential information security incidents, particularly those that could adversely affect business continuity, measures should then be put in place to either remove or reduce the risk.

Volunteers and employees must not leave portable computers, client's notes or files in unattended cars or in easily accessible areas. Ideally, all files and portable equipment should be stored under lock and key when not actually being used and overnight. Mothers records, if taken home, should be stored securely to prevent anyone else having access to the notes, procedures for safeguarding the information effectively should be locally agreed.

The introduction of this policy will place restrictions on the use of portable data storage devices for all volunteers and employees in terms of what they can use the portable devices for, and how the data must be protected when the use of a portable device is permitted. The restrictions will be to the benefit of volunteers and employees in that they will ensure that data is adequately protected in the event of any loss, which will prevent a breach of confidentiality.

Keeping information secure

- Person identifiable data must not be held on portable media, particularly memory sticks unless there is a definite need to do so and this has been approved by the Caldicott Guardian/ director responsible.
- Person identifiable data must not be sent via unencrypted email or unregistered mail.
- All portable media used by BfN needs to be logged to track its use and location.
- Where person identifiable information is held on portable media it will be encrypted.

- Consider a password-protected screensaver to prevent unauthorised access to electronic data.
- Passwords should be at least 6 characters long with a mixture of letters, upper and lower cases, numbers and symbols.
- Where general access to rooms is unrestricted, it is good practice to clear desks of all sensitive and confidential information if the rooms are left unattended for any length of time and to ensure that such information is locked securely away overnight.
- Any equipment lost or stolen should be reported immediately.
- Any new equipment needs to meet these standards and comply with a formal privacy impact assessment where necessary.

Keeping information to a good standard

We can all help maintain BfN's reputation by being careful with emails we send – pause before you hit the send button - and check you would be happy to sign your name to if it was a letter being published in the newspapers.

All BfN emails should be sent with a standard footer explaining to the recipient that you are from the Breastfeeding Network and containing an Information Governance statement. BfN emails should be retained for a minimum of 2 years.

If you are using a BfN laptop for any non-work related emails or documents, e.g. private emails, these should be stored in your email account or network folder clearly marked as 'Personal'. Spam should be deleted without opening or resending it, unauthorised software should never be used and memory sticks or other portable media devices should only be used to remove non-confidential documents unless you have been given a BfN encrypted media device.

10. Records Management

BfN will continue to develop and improve good record systems based on the Nursing and Midwifery Council Record Keeping Guidance for Nurses and Midwives as an example of best practise standards. [Link on p15]

Records should be kept accurate, written at the time an event occurred and complete i.e. all the information relating to individual mothers should be kept together, securely, in the one place.

We all have responsibility to keep the writing in all records legible, factual and complete so others can read them and because the mother may request a copy. The records need to be easy to locate. Before creating a new record make sure there is not an existing one to avoid duplication records being created.

Effective record keeping is evidence of

- showing how decisions related to support given are made
- supporting the delivery of BfN services
- supporting effective decision making and communication
- making continuity of information giving and support easier
- providing documentary evidence of services delivered
- promoting better communication and sharing of information between members of the multi-professional teams
- helping to identify risks, and enabling early detection of complications
- helping to address complaints or legal processes.

The Breastfeeding Network works in partnership with providers and commissioners of services and BfN members will be expected to be orientated to local documentation policies. BfN workers will be expected to record support given using the following principles.

Principles of good record keeping

- Handwriting should be legible.
 - All entries to records should be signed. In the case of written records, the person's name and job title should be printed alongside the first entry.
-

- In line with local policy, you should put the date and time on all records. This should be in real time and chronological order and be as close to the actual time as possible.
 - Your records should be accurate and recorded in such a way that the meaning is clear.
 - Records should be factual and not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation.
 - Records should identify any risks or problems that have arisen and show the action taken to deal with them. This should reflect the level of responsibility at which you are working and show ongoing referrals.
 - You have a duty to communicate fully and effectively with your colleagues, ensuring that they have all the information they need about the people with whom you have contact
 - You must not alter or destroy any records without being authorised to do so.
 - In the unlikely event that you need to alter your own or another person's, you must give your name and job title, and sign and date the original documentation. You should make sure that the alterations you make, and the original record, are clear and auditable.
 - Where appropriate, the person who you are supporting should be involved in the record keeping process.
 - The language that you use should be easily understood by the people you are supporting.
 - Records should be readable when photocopied or scanned.
 - You should not use coded expressions of sarcasm or humorous abbreviations to describe the people in your care.
 - You should not falsify records.
-

Confidentiality

- You need to be fully aware of the legal requirements and guidance regarding confidentiality and ensure your practice is in line with BfN's policies.
 - You should be aware of the rules governing confidentiality in respect of the supply and use of data for secondary purposes.
-

- You should follow local policy and guidelines of the organisation you are working with when using records for research purposes.
 - You should not discuss the people in your care in places where you might be overheard. Nor should you leave records, either on paper or on computer screens, where they might be seen by unauthorised staff or members of the public.
 - You should not take or keep photographs of any person, or their family, that are not relevant.
 - People in your care should be told that information on their health records may be seen by other people or agencies involved in their care.
 - People in your care have a right to ask to see their own health records. You should be aware of your local policy and be able to explain it to the person.
 - People in your care have the right to ask for their information to be withheld from you or other health professionals. You must respect that right unless withholding such information would cause serious harm to that person or others.
 - If you have any problems relating to access or record keeping, such as missing records or problems accessing records, and you cannot sort out the problem yourself, you should report the matter to someone in authority. You should keep a record that you have done so.
 - You should not access the records of any person, or their family, to find out personal information that is not relevant to their care.
-

Disclosure

Information that can identify a person in your care must not be used or disclosed for purposes other than the support you are providing without the individual's explicit consent. However, you can release this information if the law requires it, or where there is a wider public interest.

Under common law, information can be disclosed if it will help to prevent, detect, investigate or punish serious crime or if it will prevent abuse or serious harm to others.

BfN, in line with NHS guidance, has a policy for the suitable retention and timely disposal of records, see annex 5. Records relating to breastfeeding support will be recorded in the Personal Child Health Record book (Red Book) or maternity notes. In areas with funded

peer support programmes it may be necessary to have separate records describing the information and support given to mothers. For record retention purposes this ensures the records will be kept for the appropriate time.

BfN's record retention policy applies to both paper and electronic records and there will be a systematic procedure in place for the review of these records. Personal identifying information will be destroyed under confidential conditions (shredded).

Improving the quality of the information we hold is the key to improving the service we give to mothers and babies. If you have a computer account, you will be responsible for maintaining effective document management system within it, preventing unauthorised access with inherent potential for data corruption or loss and for backing up the data regularly.

11. Information Sharing

By setting standards for the effective & appropriate handling of information this Information Governance policy will help us to work with other organisations, share good practice ideas and avoid duplication through shared efforts.

12. Information Governance– annual assessment of compliance

- The Breastfeeding Network is required to complete the Information Governance Statement of Compliance (IGSoC). The IGSoC process requires that organisations undertake an annual IG assessment using the IG toolkit. [Further details on the Connecting for Health website]
- IG assessments need to be submitted annually by the 31st March each year to demonstrate standards are being improved or maintained, and will if necessary, need to be supported by action/implementation plans.
- The key requirements defined within the NHS Operating Framework are also the key requirements necessary for the IG Statement of Compliance.
- The IGSoC assessment process requires the development of an implementation plan.

Topic	Website link
<p>Breastfeeding Network is a registered Data Controller</p>	<p>Registration number Z2041090</p> <p>Security number 10821264</p> <p>The Information Commissioner's Office http://www.ico.gov.uk/</p>
<p>Information Governance Toolkit Getting Started for NHS Business Partners</p> <p>Training slides</p> <p>What you should know about Information Governance</p> <p>IG toolkit</p> <p>IG SoC for Non-NHS Organisations</p>	<p>https://www.igt.connectingforhealth.nhs.uk/Getting%20Started%20for%20NHSBP_V7.pdf</p> <p>www.igte-learning.connectingforhealth.nhs.uk</p> <p>http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/infogovleaflet.pdf</p> <p>www.igt.connectingforhealth.nhs.uk</p> <p>http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/non-nhs</p>
<p>The Care Record Guarantee</p>	<p>http://www.nigb.nhs.uk/guarantee/2009-nhs-crg.pdf</p>
<p>Caldicott guidelines</p> <p>Quick reference guide to Caldicott & the Data Protection Act 1998</p>	<p>http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5133529</p> <p>http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563</p> <p>http://www.guideweb.org.uk/section12/userfiles/docstore/pdf/INFORMATION%20GOVERNANCE.pdf</p>
<p>Data protection The Data Protection act is UK wide so the following sites apply to the whole of the UK</p>	<p>The Information Commissioner's Office</p> <p>http://www.ico.gov.uk/what_we_cover/data_protection.aspx</p> <p>Data Protection Help Line; Tel: 01625 545 745</p> <p>Email: mail@ico.gsi.gov.uk</p> <p>http://www.charity-commission.gov.uk/supportingcharities/ogs/g058a002.asp#a3</p> <p>http://www.ico.gov.uk/what_we_cover/data_protection/your_legal_obligations.aspx</p>
<p>Freedom of Information Act 2000. See also freedom of information guide on same site The Freedom of Information (Scotland) Act 2002 BfN is not included within FOI requirements</p>	<p>http://www.ico.gov.uk/what_we_cover/freedom_of_information.aspx</p> <p>http://www.opsi.gov.uk/legislation/scotland/acts2002/asp_20020013_en_1</p>
<p>The Human Rights Act 1998 effectively incorporates existing</p>	<p>http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1</p>

<p>European Court of Human Rights legislation into UK law. For example, Article 8 (The right to respect for private and family life) may be invoked if patient confidentiality is breached when a third party has sight of medical records.</p>	<p>http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG_4002951</p>
<p>The NHS Confidentiality Code of Practice</p>	<p>http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550</p>
<p>Record Keeping Guidance for Nurses and Midwives</p>	<p>http://www.nmc-uk.org/Documents/Guidance/nmcGuidanceRecordKeepingGuidanceforNursesandMidwives.pdf</p>
<p>Record retention (non health)</p>	<p>http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_093028.pdf</p>

Annex 1

The following individuals have specific duties for Information Governance in particular areas:

Staff member/ director	Specific duty
Caldicott/ IG lead	Ensure implementation of Information Governance Policy
Director: Phyll Buchanan	Oversee implementation of Information Governance Policy

LIST OF ALL RELEVANT BfN DOCUMENTS NOV 2009

Document	Issue date	Review date
BfN Code of Conduct	July 2007	July 2009

This list will be regularly updated, please replace with the latest version in Shared Files on Helpers and Supporters email list or from BfN's office, details given on front page.

Annex 2

Six Caldicott Information Management Principles

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

Annex 3

The Data Protection Act and Principles

The Data Protection Act 1998 became law in March 2000. It sets standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data.

These are summarised by 8 Data Protection Principles (listed below).

As well as information held on computers, the Data Protection Act 1998 also covers most manual records e.g. Health, Finance, Personnel, Suppliers, Occupational Health, Contractors, Volunteers, Card Indices.

Personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept 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

Principle 1 - Processed fairly and lawfully - be open, honest and clear

There should be no surprises, so ... inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with...

e.g. when formulating a research project remember to be open and transparent about what you will be doing with the information.

e.g. when working in a team, ensure that the mother is aware of who the members of the team are, and that all those involved with their care may need to see their notes.

Principle 2 - Processed only for specified purposes - if in doubt, check first!

Only use personal information for the purpose(s) for which it was obtained.

e.g. personal information on an Administration System must only be used for service use purposes - not for looking up friends' addresses or birthdays.

Only share information outside your local team, committee, elist or service if you are certain it is appropriate and necessary to do so.

Principle 3 - Adequate, relevant and not excessive

Only collect and keep the information you require. It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information “just in case it might be useful one day!”

e.g. taking both daytime and evening telephone numbers if you know you will only call in the day.

Explain all abbreviations

Use clear legible writing

Stick to the facts - avoid personal opinions and comments

Principle 4 - Accurate and kept up-to-date

Take care inputting information to ensure accuracy

How do you know the information is up-to-date?

What mechanisms do you have for checking the information is accurate and up-to-date?

e.g. each time you have contact with a Mother, they should be asked to confirm that their details are correct - address, telephone number etc. This can be simply done in a conversation with the Mother e.g. do you still live at [address], Have you changed your contact number since we last met?

- Check existing records thoroughly before creating new records
- Avoid creating duplicate records

Principle 5 - Not kept for longer than necessary

- Follow retention guidelines Check your organisation’s retention policy
- Ensure regular housekeeping/spring cleaning of your information
- Do not keep “just in case it might be useful one day!”
- Check your organisation’s disposal policy
- Dispose of your information correctly

Principle 6 - Processed in accordance with the rights of data subjects

- Subject access
- Prevention of processing

- Prevent processing for direct marketing - an end to junk mail and faxes!
- Automated decision taking
- Compensation
- Rectification/blocking/erasure
- Request an assessment

Principle 7 (Practical) - Protected by appropriate security

- Ensure security of confidential faxes by using Safe Haven/Secure faxes
- ALWAYS keep confidential papers locked away
- Do you have a clear desk policy?
- Ensure confidential conversations cannot be overheard
- Keep your password secret
- Ensure information is transported securely

Principle 7 (Organisational) - Protected by appropriate security

Your organisation should have ...

- Good information management practices
- Guidelines on IT security
- Staff training
- Confidentiality clause in employment contracts
- Procedure for access to personal data
- A disposal policy/procedure for confidential information
- Confidentiality contracts with third parties

e.g. archiving companies, cleaners, temporary staff, outside contractors e.g. Where BfN staff or volunteers are based in a children's centre

Principle 8 - Not transferred outside the European Economic Area (EEA) without adequate protection

- If sending personal information outside the EEA ensure consent is obtained and it is adequately protected
- Be careful about putting personal information on websites - gain consent first
- Check where your information is going e.g. where are your suppliers based?

The EEA comprises: EU member states: United Kingdom, France, Belgium, Germany, Denmark, Ireland, Netherlands, Sweden, Portugal, Spain, Finland plus Iceland, Liechtenstein and Norway

To sum up, remember that information must be:

Held securely and confidentially

Obtained fairly and efficiently

Recorded accurately and reliably

Used effectively and ethically

Shared appropriately and lawfully

[Annex 4](#)

Breastfeeding Network – our guarantee about client records

[Our commitments to you:](#)

1. In areas where we run peer support programmes we may record notes describing the information and support we have given to you.

If we receive a written request from you, wherever possible, we will make your records available to you free of charge if.

We will provide information in a format that is accessible to you (for example, in large type if you are partially sighted).

2. Everyone with access to your record, whether on paper or computer, must keep the information confidential.

We will aim to share only as much information as people need to know to play their part in supporting you.

3. We will not share health information that identifies you (particularly with government agencies) for any reason other than providing breastfeeding support, unless:

- you ask us to do so;
- we ask and you give us specific permission;
- we have to do this by law;
- we have special permission for health or research purposes; or
- we have special permission because the public good is thought to be of greater importance than your confidentiality.

Any information shared must comply with the Data Protection Act 1998, the NHS confidentiality code of practice and other national guidelines on best practice. There is more information about existing guidelines at:

www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/index.htm

Special permission may also be given when the public good is thought to be of greater importance than your confidentiality. This is very rare, but some situations where this might happen include:

- when a serious crime has been committed;
- when there are serious risks to the public or BfN volunteers or staff; or
- to protect children.

Other than in the most exceptional circumstances, this permission is given by the senior person in charge of protecting your privacy in each health or care organisation. (Often this person will be called the Caldicott Guardian.)

5. We will deal fairly and efficiently with your questions, concerns and complaints about how we use information about you. We have a Compliments & Complaints panel to answer questions, point people towards sources of advice and support, and advise on how to make a complaint. We will have a clear complaints procedure. We will use what we learn from your concerns and complaints to improve services.

6. We will take appropriate steps to make sure information about you is accurate. You will

be given opportunities to check records about you and point out any mistakes. We will normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you feel you are suffering distress or harm as a result of information currently held in your record, you can apply to have the information amended or deleted.

7. We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the Breastfeeding Network understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. As an organisation under contract to the NHS we must follow the same policies and use the same controls as the NHS does. We will enforce this duty at all times.

8. We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.

9. We will keep a record of everyone who accesses the electronic information the Breastfeeding Network holds about your care. You will be able to ask for a list of everyone who has accessed records that identify you, and when they did so.

There may be times when someone will need to look at information about you without having been given permission to do so beforehand. This may be justifiable, for example, if you need emergency care. We will tell you if the action cannot be justified.

10. If we find that someone has deliberately accessed records about you without permission or good reason, we will take action. This can include disciplinary action, ending a contract, firing an employee or bringing criminal charges. We will tell you if this happens.

Our commitment to you is based on the NHS Care Record Guarantee at the link below.

<http://www.nigb.nhs.uk/guarantee/2009-nhs-crg.pdf>

Records Retention Summary

This is a summary of the Minimum Retention Period for each type of non health record. Records (whatever the media) which may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. Records containing personal information are subject to the Data Protection Act 1998. These should be destroyed under confidential conditions

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- records relating to individual support (care records)
- administrative records (including personnel, estates, financial and accounting
- records, and notes associated with complaint handling;
- photographs, slides and other images (clinical & non-clinic);
- audio and video tapes, cassettes, CD-ROMs, etc
- e-mails;
- computerised records; and
- scanned documents

General records should be kept for 2 years. Directors meetings, annual auditors accounts and organisational records 30 years. Financial transactions, cheques, contracts 6 years.

Any details of breastfeeding support should be recorded in the Personal Child Health Record book (Red Book) or maternity notes. For record retention purposes this ensures the records will be kept for the appropriate time.

For further details see the link below.

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747