Blue River Home Care – Data Protection Policy

Controlled document
This document is uncontrolled when downloaded or printed

1. Aim

The aim of this policy is to instruct staff on the implications of data protection with regard to Blue River Home Care services.

This policy applies to all Blue River Home Care employees and those acting on Blue River Home Care's behalf.

2. Policy

The Data Protection Act 1998 came into force on 1st March 2000, and regulates the use of personal data, however the data is stored. The Act gives people rights over how their personal information is used and allows them to take action against abuse.

Blue River Home Care fully endorses and adheres to the principles of date protection, as enumerated in the Data Protection Act 1998.

Blue River Home Care has responsibility to ensure that data subjects have appropriate access, upon written request, to personal information relating to them

The policy sets out the over-arching guidance and principles that flow from the Data Protection Act 1998, the Caldicott Report recommendations, and the raft of other related legislation and central guidance which is used by organisations. The latter form of guidance will be used in this policy as 'best practice'.

3. Compliance with the principles of the Data Protection Act 1998 and Caldicott

Both the Data Protection Act and the Caldicott recommendations are underpinned by sets of principles which are key both to gaining an understanding of the requirements and interpreting these into working policies and procedures. This section details the principles and sets out their interpretations and policy implications.

Two key components of maintaining confidentiality are the integrity of information and its security. Integrity is achieved by safeguarding the accuracy and completeness of information through proper processing methods. Security measures are needed to protect information from a wide variety of threats.

3.1. The Data Protection Act 1998

The eight principles of the Data Protection Act 1998 apply to all staff handling personal information (on computer and manually held), and underpin all related policies and procedures. The eight principles are:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions (set out in Schedules of the Act) are met.

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date (see below).

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures (i.e., security measures) shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.2. Caldicott

The Caldicott principles and recommendations apply specifically to Customer-identifiable information, and emphasise the need for controls over the availability of such information and access to it. In particular the Blue River Home Care Managing Director has specific responsibilities to oversee an ongoing process of audit, improvement and control in line with Caldicott Guardians appointed in NHS organisations.

The six Caldicott principles, applying to the handling of Customer-identifiable information, are as follows

- Justify the purpose(s) of every proposed use or transfer.
- Don’t use it unless it is absolutely necessary, and
- Use the minimum necessary.
- Access to it should be on a strict need-to-know basis.
- Everyone with access to it should be aware of their responsibilities, and
- Understand and comply with the law.

3.3. Who may access Health Records?

Customers
A Customer may access his or her own medical records as long as the Customer has sufficient mental capacity to understand the nature of the request being made. If there is any doubt about the Customer's capacity (for example because of mental illness) an appropriate doctor should be asked to assess the Customer's mental capacity.

The Customer's Representative
A Customer may authorise another individual to have access to their records. Such authority must be in writing. The most common example is where a Customer authorises a solicitor to have access to the records. A written authority signed by the Customer must be produced before access is granted.

As before, access can only be granted where the Customer has sufficient mental capacity to understand the nature of the request and to provide the necessary authority to his/her representative.

Executors or Personal Representatives
The executor or personal representative of a deceased Customer may seek access. In addition access may also be sought by a person who may have a claim arising out of a Customer's death.
Such requests are governed by the Access to Health Records Act rather than Data Protection Act.

3.4. Fees payable

Access under the Data Protection Act
The maximum fee is £50. This fee must include all photocopying charges, fees for copy x-rays and administration charges (including any postage).
No fee is payable if the records have been added to within the 40 days preceding the request and no photocopies are provided (i.e. only inspection facilities).

Access under the Access to Health Records Act
Under the Access to Health Records Act an administration fee of £10 plus the cost of all photocopying is chargeable. There is no maximum total charge. Where the records have been added to within the 40 days preceding the request, no administration fee is chargeable.

3.5. Grounds for refusing access
The grounds upon which access may be refused are:

1. Disclosure would be likely to cause serious harm to the physical or mental health or condition of the Customer, or to any other person,

or;

2. The records contain information relating to and identifying another person unless that person has consented to the release of the information. This exception does not apply, however, where the other person is a health professional involved in the care of the Customer. An appropriate health professional (as defined) must be consulted to determine whether exception number (1) above applies. If he/she considers that it does, his/her reasons for this and the records to which it relates should be set out in writing. In any such case consideration should be given to blanking out those parts of the records to which the exceptions apply and allowing access to the remainder. It may, therefore, for example, be necessary to blank out the names of third parties or references that may be harmful.

4. Informing and getting Consent

The general interpretation of the first data protection principle is that data subjects (Customers, staff, etc) need to be informed about how their information may be used and, in some circumstances asked for their express consent.

In particular, a key implication of the first data protection principle, in conjunction with the Common Law requirement, is that individuals should be fully informed of the use to which information about them may be put and the extent to which it may be shared, and have the opportunity to make known any objections. In some circumstances this would convey the 'implied consent' of the individual.

If an individual (having been fully informed about the use of their information, including about the consequences, and having had the opportunity to object) wants information about themselves to be withheld from someone or some agency, the individual's wishes should be recorded and respected, whenever feasible.

4.1. Customer consent to disclosing

Customers generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if Customers choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited. Customers must be informed if their decisions about disclosure have implications for the provision of care.

Where Customers have been informed of:

- The use and disclosure of their information associated with their healthcare.
- The choices that they have and the implications of choosing to limit how information may be used or shared; then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that Customers understand what may happen and are content should be taken.

Where the purpose is not directly concerned with the healthcare of a Customer however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

5. Consent Issues

5.1. Competence to consent

Seeking consent may be difficult, either because Customers' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

- In the former case, extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g. providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.
- In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the Customer, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Disability Discrimination Act 1995, and may prevent consent from being gained. Support for communicating with Customers having specific disabilities can be obtained from a range of agencies, e.g.

- Royal National Institute for the Blind
- Royal National Institute for the Deaf
- Disability Rights Commission – www.drc-gb.org
- Speak ability – www.speakability.org.uk

5.2. Where Customers are unable to give consent

If a Customer is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the Customer's best interests and any previously expressed wishes, and be informed by the views of relatives or carers as to the likely wishes of the Customer. If a Customer has made his or her preferences about information disclosures known in advance, this should be respected.

Sometimes it may not be practicable to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the individual concerned is minimal.

Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Section 60 of the Health and Social Care Act 2001.

Where the Customer is incapacitated and unable to consent, information should only be disclosed in the Customer's best interests, and then only as much information as is needed to support their care. This might, however, cause unnecessary suffering to the Customer's relatives, which could in turn cause distress to the Customer when he or she later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the Customer. Decisions to disclose and the justification for disclosing should be noted in the Customer's records.
Focusing on the future and care needs rather than past records will normally help avoid inappropriate disclosures.

Such circumstances will usually arise when a Customer has been unable to give informed consent to care and treatment, and, provided the Customer has not objected, this may justify the disclosure of some information with relatives in order to better understand the Customer's likely wishes. There may also be occasions where information needs to be shared with carers in order to assess the impact of disclosures to the Customer him or herself. Such occasions are rare and justifiable only in the best interests of the Customer.

Customers are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the Customer does not object. This gives Customers the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

5.3. Explicit consent

When seeking explicit consent from Customers, the approach must be to provide:

- Honest, clear, objective information about information uses and their choices – this information may be multi-layered, allowing Customers to seek as much detail as they require.
- An opportunity for Customers to talk to someone they can trust and of whom they can ask questions.
- Reasonable time (and privacy) to reach decisions.
- Support and explanations about any form that they may be required to sign.
- A choice as to whether to be contacted in the future about further uses, and how
- Evidence that consent has been given, either by noting this within a Customer's health record or by including a consent form signed by the Customer.

The information provided must cover:

- A basic explanation of what information is recorded and why, and what further uses may be made of it.
- A description of the benefits that may result from the proposed use or disclosure of the information.

- How the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed.
- Any outcomes, implications, or risks, if consent is withheld (this must be honest, clear, and objective – it must not be or appear to be coercive in any way).
- An explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).

The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences.

5.4. The right to withhold or withdraw consent

Customers do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Where Customers are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a Customer exercising his or her right to refuse treatment.

There are a number of things to consider if this circumstance arises:
- The concerns of the Customer must be clearly established and attempts made to establish whether there is a technical or procedural way of satisfying the concerns without unduly compromising care.
- The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.

- Decisions about the options that might be offered to the Customer have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the Customer of not providing healthcare.

Every effort must be made to find a satisfactory solution. The development of technical measures that support Customer choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision making process and the choices made by the Customer must be included within the Customer's record.

6. Maintaining health care records

Blue River Home Care customers' records should be factual, consistent and accurate:

- Be written as soon as possible after an event has occurred, providing current information on the care and condition of the Customer.
- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly.

- Be accurately dated, timed and signed or otherwise identified, with the name of the author being printed alongside the first entry.
- Be readable on any photocopies.
- Be written, wherever applicable, with the involvement of the Customer or carer.
- Be clear, unambiguous, (preferably concise) and written in terms that the Customer can understand. Abbreviations, if used, should follow common Blue River Home Care conventions.
- Be consecutive.
- For electronic records, use standard coding techniques and protocols.
- Be written so as to be compliant with the Race Relations Act and the Disability Discrimination Act.

Customer records should be relevant and useful:

- Identify problems that have arisen and the action taken to rectify them.
- Provide evidence of the care planned, the decisions made, the care delivered and the information shared.
- Provide evidence of actions agreed with the Customer (including consent to treatment and/or consent to disclose information).

Customer records should include:

- Medical observations: examinations, tests, diagnoses, prognoses, prescriptions and other treatments.
- Relevant disclosures by the Customer – pertinent to understanding cause or effecting cure/treatment.
- Facts presented to the Customer.
- Correspondence from the Customer or other parties.

Customer records should not include

- Unnecessary abbreviations or jargon.
- Meaningless phrases, irrelevant speculation or offensive subjective statements.
- Irrelevant personal opinions regarding the Customer.

7. Keeping Customer information physically and electronically secure

7.1. Blue River Home Care Staff should not:

- leave laptops, medical notes, rotas or files in unattended cars or in easily accessible areas
- In the office all files and portable equipment should be stored under lock and key when not actually being used

7.2. Keeping Customers' information secure: Office Staff

For using emails securely:

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.

- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

For using faxes securely:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.

- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.

- Ring up or email to make sure the whole document has been received safely.

- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

For other security:

Shred all your confidential paper waste. Check the physical security of your premises.

7.3. Train your staff:

- ✓ so they know what is expected of them; to be wary of people who may try to trick them into giving out personal details;
- ✓ to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- ✓ not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- ✓ not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- ✓ not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service

7.4. For all types of records, staff working in offices where records may be seen must:

- ✓ Shut/lock doors and cabinets as required.
- ✓ Wear building passes/ID if issued.
- ✓ Query the status of strangers.
- ✓ Know who to tell if anything suspicious or worrying is noted.
- ✓ Not tell unauthorised personnel how the security systems operate.
- ✓ Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.

With electronic records, Blue River Home Care staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal or mobile device unattended and logged-in.

- Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
- When transferring information by email to outside of the organisation all information should be password protected, the password should then be given separately from the original email
- It is advisable not to fax personal or confidential information.

Blue River Home Care Field Based staff

For all types of records, staff working in the field where records may be seen must not:

- leave laptops, phones, tablets, medical notes, rotas or files in unattended cars or in easily accessible or viewable areas
- Staff should not normally take health care records home where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed

Rotas contain confidential information and the following is to be applied: -

- rotas or files are not to be left in unattended cars
- rotas are to be returned to the office for shredding
- All rotas if being emailed to workers should be password protected

8. Common Law and disclosure in the Public Interest

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form, except as originally understood by the confider, or with his or her subsequent permission.

There are exceptions to the duty of confidence that may make the use or disclosure of confidential information appropriate. Statute law requires or permits the disclosure of confidential Customer information in certain circumstances, and the Courts may also order disclosures. Case law has also established that confidentiality can be breached where there is an overriding public interest.

9. Human Rights Act 1998

Article 8 of the European Convention on Human Rights, which is given effect in UK law by the Human Rights Act, establishes a right to 'respect for private and family life'.

This may be open to some interpretation in points of detail by the courts in years to come, but it creates a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records. It underpins the Confidentiality Model presented in this code of practice. There are also more general requirements in relation to actions having legitimate aims and being proportionate to the need.
Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality 26 should satisfy Human Rights requirements.

10. Review

This policy and procedure will be reviewed in light of any changes to national legislation or every twenty four months, whichever is sooner