

BRADWELL HALL NURSING HOME LTD

Old Hall Drive, Bradwell, Newcastle under Lyme, Staffordshire ST5 8RQ

In association with

Trentham House Care Home

Chivelstone Grove, Trentham, Stoke-on-Trent, ST4 8HN

INFORMATION GOVERNANCE CODE OF CONDUCT **DATA SECURITY AND PROTECTION**

All employees working in Bradwell Hall Nursing Home are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998.

This means that employees are obliged to keep any personal identifiable information strictly confidential (e.g. resident and employee records). In addition, where employees are using resident or staff listings these documents should be treated with the same degree of care as they may contain sufficient information to identify individuals.

This Code of Practice has been produced so that all are clearly made aware of their responsibilities and their legal duty of confidentiality in respect of information that they may have access to in the course of their duties, and to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information gained during their employment by Bradwell Hall Nursing Home.

Definition of Confidential Information

Confidential information can be anything that relates to patients, staff, volunteers, bank and agency staff, locums, student placements, their family or friends, however stored or used. It also refers to corporate information that is sensitive and not intended for the public domain.

It can take many forms including medical notes, audits, employee records etc. Information may be held on paper, floppy disc, USB pen, CD, computer file or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, tablets, USB pens, mobile phones, dictaphones and digital cameras.

Person-identifiable information is anything that contains the means to identify a person (e.g. name, address, postcode, date of birth, national insurance number etc.) Even a visual image (e.g. a photograph) may be sufficient to identify an individual.

Any information that you use at work, even something as simple as a resident's name and address, you should consider to be sensitive and take care to protect it.

Requests for Information on Residents

- Never give out information on residents or staff to persons who do not "need to know".
- All requests for identifiable information should be on a justified need.
- Agreement to share information should be obtained from the resident.
- In the case where a resident is unable to give consent, a 'best interest' decision should be made on behalf of the resident.

If you have any concerns about disclosing/sharing resident information you must discuss this with your manager or someone with similar standing if they are not available.

Telephone Enquiries

If a request for information is made by telephone

- Always try to check the identity of the caller, and
- Check whether they are entitled to the information they request
- Take a number, verify it independently and call back if necessary

Remember that even the fact that a person is in Bradwell Hall Nursing Home, or a member of staff, is confidential. If in doubt consult your Manager.

Any suspected bogus telephone call should be notified to your manager at the time.

Carelessness

- Do not talk about residents in public places or where you may be overheard.
- Do not leave any medical records or confidential information lying around unattended.

- Make sure that computer screens, or other displays of person identifiable information, cannot be seen by the general public.

Use of Mail

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven: and not to a department, unit or an organisation.

Faxing / Emailing Confidential Information

- Remove all staff/resident identifiable data from any faxes/emails, unless you are faxing/emailing to a known secure and private area.
- Faxes/Emails should always be addressed to named recipients.
- Always check the number/email address to avoid sending to an incorrect recipient.

Storage of Confidential Information / National Data opt-out Service

Paper-based confidential information should always be kept secure, and should be locked away when unattended. Confidential information should not be left in any building/office that is going to remain un-occupied for a long period of time. In line with the national data opt-out service, please contact the registered manager or senior member of staff if you would like your personal data destroyed. Please be aware that some personal data has to be kept by law and is always be kept securely.

Disposal of Confidential Information

Paper-based person-identifiable information should be shredded. Discs containing confidential information must be destroyed by either shredding in an appropriate shredder or damaging the surfaces of the media before disposal. Computer hard disks and USB memory sticks should be destroyed.

Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone. Passwords should not be written down.

Non-Compliance

Non-compliance with this Code of Conduct by any person working for Bradwell Hall Nursing Home may result in disciplinary action being taken, and may lead to dismissal for Gross Misconduct.