Confidentiality Policy

Policy Data Sheet

Policy Name:	Confidentiality
Document Reference:	BLG0012
Version Number:	10
Ratified By:	Executive Team
Exec Team Ratified Date:	May 2024
Review Period:	3 years
Review Date:	May 2027

Contents:

ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.

Confidentiality Policy

1. Aim of the Policy

The Big Life Group is committed to good practice in all aspects of service delivery and employment practice. Key to achieving this is to have a clear policy on confidentiality that applies to all staff members and volunteers; confidentiality is essential to safeguard people including individual clients, employees, and volunteers, and the business to ensure a high standard of practice.

This policy aims to ensure that all staff and volunteers follow processes that ensure that individuals' and the businesses' confidentiality is safeguarded. The policy will adhere to (1) the various professional codes of conduct (e.g. the NHS Confidentiality Code of Practice) (2) the law (i.e. common law duty of confidentiality) and (3) the Caldicott Principles. These must be observed to protect both the individual client and also the integrity of the various professionals involved.

2. Scope of the Policy

Issues of confidentiality need to be considered in relation to safeguarding personal information relating to service users, staff members and volunteers, and enabling appropriate information sharing.

Confidentiality also applies to business information including contractual, financial and governance information for example. This policy contributes to the Information Governance Framework and is related to a number of associated policies (see Section 8)

This policy is aimed at staff members, volunteers, and 3rd party colleagues working within the group. *Failure to work within this policy will treated as a disciplinary matter and may also lead to a professional governing body being informed if appropriate*.

3. Roles and Responsibilities

Board
The ultimate responsibility for protecting the confidentiality of personal information and enabling appropriate information rests with the Board of Directors. The board has responsibility for ensuring a Caldicott Guardian is appointed. The board receives assurance reports from the Risk and Quality Committee.

Caldicott Guardian
The Caldicott Guardian in The Big Life Group is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing; the guardian is a member of the Board, Clinical and Service Governance Board, and

the Executive Team. All staff members, volunteers, and service users must know how to contact the Caldicott Guardian with concerns, or for advice.

Quality Committee
Attended by the Information Governance Lead (DPO) and Caldicott Guardian. Reviews staff training,and reviews all serious incidents involving actual or potential loss of data or breach of confidentiality.

Executive Team
Responsible for the day-to-day operation of the group and ensuring that staff, systems and sub-contractors comply with the requirements of the Confidentiality Policy. Responsible for appointing the Data Protection Officer/Information Governance Lead.

Data Protection Officer/Information Governance Lead
Provides assistance to monitor internal compliance, informs and advises on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. Ensures the Framework and Policies are updated in line with best practice and learning; and participates in the investigation and reporting of information incidents.

Managers
Managers are responsible for ensuring that their staff understand and comply with this confidentiality policy, and receive appropriate training

Staff
All staff members are required to comply with this policy, and undertake training as directed

Sub-contractors and third parties
Are required to comply with this policy, associated policies and business-level operational procedures and to report any incidents as required. This forms part of the initial due diligence and service level agreement.

4. Basic Principles of Confidentiality

Duty of Confidence

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will not be further disclosed without appropriate controls.

Within the group, all personal information pertaining to staff members, volunteers, and clients, is deemed to be confidential if the information was disclosed for work purposes or the purpose of seeking support. As a guide, the following is a list of information that is regarded as confidential; this list is not exhaustive

- Client/Service User Notes
- Client/Service User emails/contact details
- Staff/Volunteers addresses and personal phone numbers

- Absence records including doctors certificates
- Details pertaining to disciplinary proceedings
- Staff supervision notes

Confidential information pertaining to the business may include:

- Financial information
- Contracts
- Non-disclosure agreements

Confidentiality information is not secret in the sense that it can never be disclosed to anyone else. However, information sharing must be appropriate.

Caldicott Principles

In 1997 Dame Caldicott undertook a review into the processing of personal information within the NHS. Following this the Caldicott Principles were developed to safeguard the confidentiality of clients' information and enable appropriate information sharing. These principles apply to all confidential information, and outside the NHS as well as within it. The principles are:

- Justify the purpose(s) for using/sharing confidential information
- Only use confidential information when absolutely necessary
- Use only the minimum confidential information that is required
- Access to confidential information should be on a strict need to know basis
- Everyone should be aware of and understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Caldicott Guardian

One recommendation from the Caldicott report was that every organisation should appoint a board member or senior staff member to the position of Caldicott Guardian.

The Caldicott Guardian is responsible for protecting confidential information and enabling appropriate information-sharing.

Within The Big Life Group, the Caldicott Guardian is fay.selvan@thebiglifegroup.com

If staff members, volunteers, clients, and members of the public have concerns about the way confidential information is being used within the Group, and do not feel these concerns have been satisfactorily addressed, it is essential that they are made aware of how to contact the Caldicott Guardian.

5. Information Sharing

Sharing confidential information must be undertaken in accordance with Caldicott Principles (see above).

Access

Within the group, confidential information must only be accessed on a need-to-know basis (i.e. the information is only accessed by people who need to access it to undertake a work function). Where possible, technical (see access control policy for further information) and physical measures should be used to ensure confidential information can only be accessed by those who need to access it. However, access requirements may be complex and dynamic and the use of technological controls to restrict access can lead to other risks.

Therefore, all staff members/volunteers have a responsibility only to access confidential information for the purpose of performing work related duties.

Consent

In most cases confidential information can be shared only with the explicit consent of the person who it pertains to.

Within data protection legislation, explicit consent requires the following conditions are met.

The person must

- understand what information is to be shared and to whom, and the purpose of sharing the information
- give consent freely – (i.e. they must not be led to believe that there would be any disadvantage of not giving consent over and above that arising directly from the information not being shared)
- have capacity to understand what they are being asked to agree to
- understand that they may withdraw consent in the future

Consent does not always need to be given in writing, but it must be expressly confirmed in words (given explicitly), rather than by any other positive action. It is essential that when verbal consent is gained, a record of the decision is made in the person's record.

Sharing without Consent

There are situations where consent is not required to share confidential information. It is essential that all staff members, volunteers, and service users understand when their personal information can be shared without consent.

Sharing confidential information without the consent of the person who divulged the information is often described in shorthand as 'breaking confidentiality'. It is good practice and in line with Big Life Values to be open and honest to people when it is

necessary to break confidentiality; however, there will be situations when this is not possible, these situations are as follows.

1. It is not possible to inform the person and reasonable attempts have been made to inform them.
2. We have been instructed not to inform the person
3. It is assessed that informing the person will greatly increase the risks to the safety of one or more individuals.

It may be necessary to break confidentiality in the following situations

1. Someone's life or personal safety is considered to be at risk
2. Duties/responsibilities that arise from the services being provided, or professional code of practice.
3. Safeguarding children or a vulnerable Adult
4. It is a requirement of the law
5. There is an overriding public interest to share the information

The main **public interest** justifications for the disclosure of information include:

- public accountability and monitoring purposes
- serious risk to public health
- the prevention, detection or prosecution of serious crime
- disclosures to professional regulatory bodies (e.g. investigations of professional misconduct)

Scenarios 1 and 2
It is essential that all services/businesses have robust operational procedures and staff training to enable operational managers to make decisions about breaking confidentiality.

Scenario 3:
For guidance on information sharing relating to safeguarding children/young people, refer to the Safeguarding Children and Young People's Policy

For guidance on information sharing relating to Vulnerable Adults, refer to the Safeguarding Adults policy

Scenario 4:
An Executive Director must authorise disclosures that fall into this category. All such requests must be supported by the relevant paperwork outlining the legislation being applied. The paperwork must also include the credentials of the official making the request (e.g. sent on letter headed paper or from an official email address). The Information Governance lead must also be informed. The Information Governance Lead/Data Protection Officer is responsible for storing appropriate records of the disclosure.

Scenario 5:

The Caldicott Guardian must authorise disclosures that fall into this category; when the Caldicott Guardian is absent an Executive Director can deputise. All such requests must be in writing with the appropriate credentials. The Information Governance Lead/Data Protection Officer must also be informed. The Information Governance Lead/Data Protection Officer is responsible for storing appropriate records of the disclosure

6. Safeguarding Confidentiality

Appropriate information security arrangements must be in place to safeguard written or electronic confidential records (see associated policies specifically **Information Governance Framework** and **Keeping Records and Data Protection Policy**).

Staff should be careful not to inadvertently share information in response to telephone calls or emails from colleagues (internal or external) who do not need to know. If a request for information is made by email or telephone, staff should check the person's name, number and agency and ask them to put their request in writing on letterhead paper.

Where services operate from a public access venue, it should be made clear to clients that personal information does not need to be given in a public area. Where possible, telephone calls should be passed directly to the member of staff who would most appropriately deal with the enquiry. If this is not possible, then a message should be taken, and stored securely until passed to the relevant staff member. When the message is confidential it should be marked **Private & Confidential**, and only viewed by the intended recipient.

Clients who phone an office should be made aware that they do not have to give a lot of personal information over the phone, especially if they cannot speak to the most appropriate person. If a call is urgent and the relevant member of staff is not available, brief details should be taken then referred to the relevant line manager, or another member of the management team.

All mail received should be passed to the appropriate member of staff. Mail marked **Private & Confidential** should be passed, unopened, to the member of staff concerned. If the member of staff is on leave or where an envelope is marked **Private & Confidential or Personal** but is not addressed to a named worker, it should be passed to a senior manager

Unless authorised by an Executive Director, email messages sent to or from a mailbox of the organisation should only be read by the sender and intended recipients. Anyone receiving a message that they suspect has been sent in error should contact the sender for clarification before reading the message.

7.Confidentiality Policy

Clients will be made aware of this policy, and it will be made available on request. The confidentiality policy is available to other agencies and individuals upon request.

The confidentiality policy is a key part of the induction training received by all members of staff. This is reinforced through one to ones, training, annual review and other methods.

Breach of the confidentiality policy may, in serious cases, constitute gross misconduct and will be dealt with in accordance with disciplinary procedure and serious cases may result in dismissal, and professional bodies being informed..

8.Associated Policies

- Information Governance Framework
- Keeping Records and Data Protection
- Information Security
- IT, Email, social networking policy
- Serious Untoward Incident and Incident
- Safeguarding
- Access Control