focus
independent adult social work

Confidentiality Policy

Version 2.0

Heritage House, Fisherman's Wharf, Grimsby, DN31 1SY

Contents

1. PURPOSE AND SCOPE

This Policy sets out focus' commitment to the confidentiality of client and staff information and its responsibilities with regard to the disclosure of such information. It also incorporates the responsibilities of staff to ensure confidentiality with regards to any sensitive information including commercially sensitive information.

All employees working with focus are bound by a legal duty of confidence to protect personal information they come into contact with during the course of their work.

The Policy is also to protect staff by making them aware of the correct procedures for maintaining confidentiality of client information so that they do not inadvertently breach any requirements of law and/or good practice. This includes partnership working and in accordance with the Integrated Urgent Care (IUC) Alliance Information Governance Management Framework (IGMF).

This Policy seeks to ensure that all Personal Information will be:-

- Obtained by appropriate and fair methods
- Obtained for specific purposes & used only for those purposes
- Shared only with the necessary consents
- Accurate and up to date
- Relevant for requirements and not excessive
- Not kept for longer than necessary & then destroyed appropriately
- Protected against loss or disclosure
- Treated as confidential at all times

All Sensitive information will be:-

- Kept and handled confidentially, whether the information has been received formally, informally or discovered by accident

This Policy applies to all person identifiable information, whether written, computerised, visually or audio recorded or any other medium.

This Policy applies to all members of staff, Students/Placement/Agency staff, volunteers, contractors and sub-contractors and any other person representing or acting on behalf of focus.

2. LEGAL FRAMEWORK

The work of focus requires the collection, use and disclosure of personal information for a number of purposes. Much of this information is of a sensitive nature and all of it is subject to a legal and statutory framework that addresses issues of confidentiality, which include:-

- Common Law Duty of Confidence – requires that the public expectations of confidentiality be respected
- The Human Rights Act 1998 – Article 8 guarantees the right to respect for privacy and family life, home & correspondence
- The Data Protection Act (2018) – requires that any personal information collected by and used within the SWP be processed fairly and lawfully
- General Data protection Regulation (GDPR) – requires that organisations adhered to the rights of individuals and the legal basis for processing data
- Caldicott Report 1997 – identifies the need to ensure that confidentiality is respected throughout the process of care
- The Public Interest Disclosure Act – which has exemptions for specific kinds of disclosure by employees, such as the raising of concerns of practice
- Computer Misuse Act 1990
- Professional Codes of Conduct / Professional Standards for all health and social care professionals

3. DEFINITIONS

Personal Information: Information relating to a living person which identifies an individual either on its own or together with information that is in focus' possession or that is likely to come into its possession.

Sensitive Personal Information : Information concerning an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sexual life, commission or alleged commission of any offence or proceedings for any offence committed or alleged to have been committed.

Sensitive Information:

- Organisational information which could be used to damage focus or its reputation or threaten the security of property, buildings or staff. Tenders and quotations for services and work.

4. DUTIES

4.1. Caldicott Guardian/Chief Executive

The Chief Executive has overall accountability for ensuring that there are appropriate arrangements in place for maintaining the confidentiality of information at all times; that any disclosures are for legitimate purposes and conform to this Policy and other legal requirements.

As Caldicott Guardian, the chief executive should actively support and facilitate appropriate information sharing and advise on the options for lawful and ethical information processing. The Caldicott Guardian is responsible for maintaining this Policy and providing advice to members of staff and the Board on the issues covered within it. The Caldicott Guardian is responsible for ensuring that national and local guidelines are in place and for overseeing the arrangements for the use and sharing of person identifiable information.

4.2. Senior Information Risk Officer (SIRO)/Head of Business & Governance

The Head of Business & Governance is responsible for ensuring that there are robust governance frameworks in place to continuously check out and improve confidentiality and security procedures governing access to and storage of personal information.

The Head of Business & Governance, via the Central Business Unit, is responsible for ensuring that all new starters are made aware of their responsibilities and obligations in respect of client confidentiality during their induction period and are fully aware of any consequences should confidentiality be breached.

The Head of Business & Governance is responsible for reviewing and acting upon appropriate Information Asset Register (IAO) recommendations for the protection and integrity of personal and confidential information where practically and financially possible.

4.3. Data Protection Officer/Head of Information and Security

The Head of Information & Security is responsible for monitoring compliance with the GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits; registering information assets through the development of an Information Asset Register (IAO) for review by the SIRO and focus board; providing risk based advice.

The Head of Information and Security is responsible for ensuring Data Protection Impact Assessments are undertaken on projects relating to the collection, storing and sharing personal information.

The Head of Information & Security is responsible for providing a service to clients to access their own records in line with the law and focus' Subject Access Request Procedure

The Head of Information and Security is responsible for ensuring all relevant data protection and security policies, procedures and privacy notice are up to date and

available on the public website in accordance with data protection laws and transparency.

The Head of Information & Security is responsible for ensuring that access to electronic and manual confidential information is strictly controlled within their system. They will be responsible for monitoring access attempts in order to highlight potential areas for concern, e.g. regular access attempts by the same individual. They will be responsible for ensuring that confidentiality audits and subsequent recommendations are complied with within the specified timescales.

4.4. All Supervisory Staff

All Supervisors have a duty to ensure that their staff are aware of their responsibilities to protect the confidentiality of client information. Supervisors are also responsible for the dissemination and implementation of this Policy to all their staff members.

4.5. All Staff

All staff are individually responsible for compliance with this Policy and risk disciplinary action if they are found to have disclosed information outside of the boundaries of this Policy which should be documented. All staff should be aware of their responsibilities and obligations to respect client confidentiality. In addition, all professional health and social care staff are bound by their existing professional ethical principles of confidence and codes of conduct as set out by the various bodies.

5. INFORMATION SHARING

Information will only be shared with partner agencies and other organisations within defined protocols and where the individual has given consent to the information being shared. As it may be impractical to obtain consent every time information needs to be shared, clients must be informed and understand that some information may be made available to other partner agencies involved in their care.

If a client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:-

- They can be justified in the public interest (usually where disclosure is essential to protect the client, or someone else, from risk of significant harm)
- They are required to by Law or by order of a Court
- Where there is an issue of child protection

All personal information will be shared with the individual unless the provisions of the Data Protection Act 2018/GDPR exclude access, (see 'Data Protection Act 2018 & GDPR).

Personal information relating to deceased individuals will continue to be treated as confidential and will not be disclosed without justification. The privacy and wishes of relatives will be taken into account when considering the appropriateness of such disclosures. Wishes expressed by the individual prior to their death will be respected and in line with the Access to Health Records Act 1990.

Where there are concerns or queries relating to information sharing, advice should be sought from either the Caldicott Guardian or focus' designated Data Protection Officer (DPO) (Head of Information & Security).

6. PROTECTION OF PERSONAL INFORMATION

Staff must guard against breaches of confidentiality by protecting information from improper disclosure at all times. Staff should be aware that such disclosure can be by any means, e.g. electronic or paper, telephone, face to face or social media.
Any files or papers relating to clients should not be left unattended or left where other members of staff / the public can see them. Access to rooms and offices where paper files and/or computer terminals are present should be controlled.
Any client information taken outside of focus buildings must be appropriately protected at all times. Individuals take full responsibility for the confidentiality of files in their possession.

Face to Face
Staff should not discuss clients or client issues where the conversation could be overheard. Wherever possible, any meetings / consultations with clients should be in private. The same approach should be adopted for discussions relating to commercially sensitive information such as tender responses and quotations.

Telephone
Confidential information will not be disclosed over the telephone unless prior confirmation regarding the identity of the caller has been made and all necessary consents obtained. Any such disclosures will be recorded on the client's file, (SystmOne). Where relatives telephone on a client's behalf, all effort should be made to speak to the client themselves. The assumption should not be made that a caller knowing the answer to some key qualifying questions, e.g. date of birth of the client, is genuinely a relative. Where there is doubt regarding the identity of a person requesting the information, guidance should be sought from a supervisor. If advice is not immediately available, then the information should not be disclosed. If the caller claims to be from another organisation, that organisation's switchboard number (not a direct line number) should be called to check that the caller is from that organisation.

Post
Post marked 'confidential' will only be opened by specifically designated staff. Post marked 'addressee only' will be opened by the named recipient, or by their line manager in the event of long term absence.

Computers
Client information must only be stored on focus equipment and not on personally owned laptops, home desk computers. IPads or other electronic media.

Client data should never be saved to hard drives of PC's due to the risk of theft and breach of confidentiality.

Staff should log off their laptops whenever they are not at their desk and should be aware at all times of who may be in the vicinity of their computer screen when working at it, e.g. contractors, visitors etc.

E-Mail
In line with Safe Haven principles, transfer of personal information by e-mail should be avoided unless the information is encrypted. NHSmail is an approved e-mail service for securely exchanging data between NHSmail users. Unless both sender and recipient are NHSmail users, a risk assessment should be undertaken by the Data Protection Officer/Head of Information & Security and any attachments encrypted.
Personal identifying information should NEVER be contained within the subject line of an e-mail.

7. STORAGE AND DISPOSAL OF PERSONAL INFORMATION

Appropriate arrangements for the safe storage and disposal of all personal information (both hard copy and electronic) must protect confidentiality and be in line with focus' Destruction and Retention Policy

Files (hard copy and electronic) will not be retained for longer than the agreed retention period and confidential material will be destroyed using an appropriate method once it is no longer required, see 'Disposal of Confidential Waste' Business Procedure.

8. BREACHES OF POLICY

Breaches of the Confidentiality Policy may constitute Gross Misconduct and will be investigated under focus' Disciplinary procedure. Note: The unauthorised disclosure of personal information is an offence under the Data Protection Act 2018/GDPR.

9. MONITORING COMPLIANCE AND EFFECTIVENESS

All actual or potential breaches of confidentiality will be investigated and monitored in line with focus Incident and Accident Reporting Procedure. focus' Professional Practice Governance Committee will monitor all such incidents.

10. POLICY REVIEW

This policy will be reviewed within a three year period as part of a rolling programme unless there are any changes in legislation

11. INTERNAL REFERENCES

- Information Governance Management Framework (IGMF)
- Information Governance Policy
- Information Security Policy
- Data Protection Policy
- Staff Code of Conduct
- Social Media Policy and Guidance
- Destruction and Retention Policy
- Incident and Accident Reporting Procedure

12. IMPACT ANALYSIS

This policy will pay due regard to the following impacts:

12.1. Equality

In developing this policy, an equality impact assessment has been completed (See focus IGMF). A full equalities impact assessment was deemed not to be required. This is because the policy is formatted in a way that is easy to read and can be made available on request in other formats and in other languages from the author of this framework. Arrangements can be made for members of staff with disabilities who wish to access information in a different format.

As a result of performing the analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage.

12.2. Sustainability

The policy will pay due regard to any requirements during their activity and tendering of the sustainability Impact Assessment, undertaking where appropriate.

12.3. Bribery Act 2010

focus will need to fully and be careful to ensure that under the Bribery Act 2010, it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper. It is therefore, extremely important that staff adhere to this and other related policies and documentation outlined within their organisation, such as a Gifts and Hospitality Policy when considering whether to offer or accept gifts and hospitality and/or other incentives.

13. REFERENCE MATERIAL

External

- Current Data Protection Legislation
- General Data Protection Regulations (EU) 2016/679
- The Computer Misuse Act (1990)
- Human Rights Act 1998 (Specifically Article 8)
- Care Act 2014
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- The Public Records Act (1958)
- NHS Code of Practice, The Common Law Duty of Confidentiality
- Mental Capacity Act (2005)
- NHS Information Governance: Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- NHS England: Everyone Counts: Planning for Patients 2014/15 to 2018/19
- NHS Digital: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- National Information Board and DH: Personalised Health and Care 2020
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice