Confidentiality Policy and Procedures (Northern Ireland)

Policy Lead	Mayvelyn Talag Registered Manager NI
Authors	Florence Governance Team
Ratified	Florence Leadership Team 19th January 2024
Policy Number	FNI05
Version Number	1.0
Date of issue	30th January 2024
Date to be reviewed	30th January 2027
The controlled version of this document is stored on the Policy Portal on Notion. **Not controlled once printed**	

Table of Contents

1. Introduction

All healthcare service providers have an ethical, legal and contractual duty to protect service user confidentiality. Information sharing can help to improve the quality of care and treatment, but it must be governed by the legal and ethical framework that protects the interests of service users.

Service users entrust the healthcare providers with their personal information and expect us to respect their privacy and handle their information appropriately. Everyone should seek to ensure that protection of service user confidentiality on collecting and sharing information is built into all healthcare to provide safe and effective care.

1. Policy Statement

This policy outlines the guiding principles for information sharing, based on legal and ethical requirements. It aims to provide a framework for the secure sharing of service user identifiable information between partner organisations and also covers wider issues of disclosing information to third parties.

This policy sets out the standards and practice relating to confidentiality applicable to all employees who work for a healthcare service. This policy should be read in conjunction with all of Florence's policies and procedures, but in particular the Data Protection and Records Management Policy and Procedures (Northern Ireland).

2. Scope

This policy applies to all individuals associated with Florence, including but not limited to employees, care professionals, service users, families, advocates, commissioners, external health professionals, and stakeholders.

The scope extends to all interactions involving confidential information within the organisation, whether related to service delivery, employees, clinical governance, health and safety, technology and innovation, continuous improvement initiatives, financial performance, or addressing risks and challenges.

All employees and stakeholders are expected to adhere to the principles outlined in this policy to ensure legal compliance, ethical conduct, and the protection of personally identifiable information.

3. Definitions, Roles and Responsibilities

Personal confidential data: information that relates to an identified or identifiable individual. This data should not be processed without a clear legal basis. Personal confidential data should only be disclosed with consent or under statute, and any disclosure must always be limited and accompanied by a contractual agreement that mitigates the risk of misuse and inappropriate disclosure. The contractual agreement needs to set out, as a minimum, the legal basis for the data flow, the purposes to which the data can be put, the safeguards that should be in place to protect data and how the public are informed about these.

Service User identifiable information: all personal health information is held under strict legal and ethical obligations of confidentiality. Information given in confidence should not be used or disclosed in a form that might identify a service user without their consent. Service user identifiable information includes:

- Name
- Address
- Full postcode
- Date of birth
- NHS number
- National Insurance Number
- Pictures, photographs, videos, audiotapes or other images of the service user, as even a visual image (e.g. photograph) is sufficient to identify an individual.
- Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Non-person-identifiable information: can be classed as confidential, such as confidential business information (e.g. financial reports and commercially sensitive information, e.g. contracts, trade secrets and procurement information) which should also be treated with the same degree of care.

Special categories of personal information: previously known as 'sensitive' personal data, defined by the Data Protection Act 2018 as refers to personal information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Processing of genetic data
- Biometric data (for the purpose of uniquely identifying a natural person)
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation.

Care Professionals - Anyone on the Florence platform that carries out work on behalf of Florence in other organisations, for example registered nurses and care assistants.

Central Team - All direct employees of Florence that are not care professionals working through the Florence platform

Chief Technology Officer (CTO)- serves as the Data Protection Officer. Their responsibilities include:

- Developing and implementing data protection policies and procedures.
- Monitoring and ensuring compliance with data protection laws and regulations.
- Conducting risk assessments and implementing appropriate security measures to protect data.
- Providing training and guidance to staff on data protection best practices.
- Handling data breach incidents and coordinating the necessary actions to mitigate risks.

Chief Operating Officer (COO) serves as the Senior Information Risk Owner (SIRO) and Registered Person in Northern Ireland. Their responsibilities include:

- Taking overall responsibility for information risk management within the organisation.
- Establishing and maintaining an effective information risk management framework.
- Assessing and managing information risks associated with the agency's operations.
- Ensuring that appropriate controls are in place to protect sensitive information.
- Collaborating with other stakeholders to address information risks and ensure compliance with relevant regulations.

Service User - a person who uses health and/or social care services. Sometimes known as a “patient”, “service user” or “person in care”.

Employees - everyone employed by Florence directly and indirectly, including care professionals using the platform and the central team.

Regulation and Quality Improvement Authority (RQIA) - is the independent body responsible for monitoring and inspecting the availability and quality of health and social care services in Northern Ireland, and encouraging improvements in the quality of those services.

Registered Manager - is responsible for ensuring that this policy meets the needs of regulators in Northern Ireland.

Quality and Governance Director - serves as the Data Protection Guardian for Northern Ireland. Their responsibilities include:

- Ensuring compliance with data protection laws and regulations in Northern Ireland.
- Overseeing the implementation of data protection policies and procedures.
- Providing guidance and support to staff regarding data protection matters.
- Conducting regular audits to assess data protection practices and identify areas for improvement.

4. The Position of Florence on Confidentiality

Confidential information will not be used for a different purpose or passed on to anyone else without the consent of the information provider.

- There may be occasions when it could be detrimental to the Individual or to another Individual if this principle is strictly adhered to.
- There is a recognition that breaches of confidence are often unintentional. They are often caused by employee conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences could be equally serious for all concerned.
- Florence will ensure that personally identifiable information will always be held securely and, when used, treated with respect. This rule will apply regardless of where the information is held.
- Although the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act no longer apply to identifiable data that relate to a person once they have died, we respect that any duty of confidence established prior to death continues after a Individual has died.
- All information regarding the service users we support through third parties will be treated with respect and integrity.
- We will be transparent in our approach to ensure that anyone associated with Florence (whether an Individual, an employee or a visitor) is fully aware of how, what, when, who and why we share any information about them and source their agreement before doing so.

All relevant employees will be bound by their professional code of ethics issued by their relevant licensing body, such as The Nursing Midwifery Council (NMC) and Northern Ireland Social Care Council (NISCC).

5. Procedures

Florence will detail with transparency how confidentiality is managed with Individuals, employees and others at the earliest opportunity and seek their agreement, e.g. through existing systems such as recruitment and Florence assessment processes.

Best Practice for Protecting Confidentiality

It is all employees' responsibility to make sure that they follow the measures set out below to protect the confidential information that they have gained privileged access to because of their role. Responsibility starts when information is received and continues when it is used, stored, shared with others and destroyed. This applies to both spoken and written information:

- Keep accurate, relevant records
- Record and use only the information necessary
- Access only the information needed
- Keep information and records physically and electronically secure and confidential (e.g. leave your desk tidy, take care not to be overheard when discussing cases and never discuss cases in public places)
- Follow Florence's guidance when using removable devices, such as laptops, smartphones and memory sticks (refer to Data Protection and Record Keeping policy), keep your usernames and passwords secret and change your passwords regularly
- Follow Florence's guidance before sharing or releasing information (including checking who a person is and that they are allowed access to the information), and when sending, transporting or transferring confidential information
- Make information anonymous where possible
- Keep and destroy information in line with local policy and national guidelines

- Always report actual and possible breaches of security or confidentiality as a matter of priority.

Best Practice for Keeping service user Records Secure

For all types of records, employees 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:

- Stored securely within the clinical environment or 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
- Held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity, though not indicating the reason for sensitivity, and permitted access, and the availability of secure means of destruction (e.g. shredding) are essential

With electronic records, employees must:

- Always log-out of any computer system or application when work on it is finished
- Not leave a terminal unattended and logged-in
- Not share logins with other people. If other employees have a need to access records, then appropriate access should be organised for them
- 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 you (e.g. children's or pet's names or birthdays)
- Always clear the screen of a previous service user's information before seeing another
- Use a password-protected screensaver to prevent casual viewing of service user information by other

Best Practice When Sharing Service User Information

The central team at Florence should never see service user information, however care professionals working in the service will as part of their responsibilities while on assignment and should follow the following guidance as well as any policy in the organisation they are working within.

Consent to share information must be sought from service users in a sensitive manner. At all times the rights, interests and dignity of the service user must be respected. Service users must have the opportunity to discuss any aspects of information sharing that are specific to their treatment and personal circumstances, for example:

- Inform service users of how information will be used before they are asked to provide it. This includes informing service users of the kinds of purposes for which information about them is collected, and the types of people and agencies to which information may need to be passed, such as clinicians
- Consent to share information must be recorded in the service user's clinical record and should be sought at the earliest opportunity.
- Once consent to share personal information has been obtained, it will be assumed to continue unless the service user withdraws consent but will be limited to the purposes for which consent was given
- A service user's case file or other personal record should always be checked for evidence of consent before personal information is shared with another agency
- Consent may be verbal or written. Service users can change their choice about their consent at any time
- Consent, whether implied (when a service user accepts a service) or explicit (when a service user indicates consent), must always follow the effective involvement of service users
- Explicit consent is best practice and should become the norm as better-informed service users share in decisions about the uses of their information.

Legal Considerations

Under common law, employees are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of a serious crime and/or to prevent abuse or serious harm to others where they judge, on a case-by-case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual service user concerned and the broader public interest in the provision of a confidential service.

Confidentiality must not be confused with secrecy. Consent to share information should be sought, but if this is not possible and others are at risk, it may be necessary to override the requirement. It is inappropriate for employees/agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly those situations where other people may be at risk.

Sharing common law confidential information without consent for purposes other than direct care

There may be circumstances where it is not practicable to use de-identified information or to get consent and, in these cases, confidential information may be shared but only if there is a legal basis for the information sharing. Requirements for consent should be considered against each of the following criteria:

Legal Requirement: the law requires clinicians to disclose information irrespective of the views of a service user (e.g. if service users contract certain notifiable diseases. The Data Protection Act requires that the service user be told about the disclosure).

To protect a service user's vital interests: for example, where a healthcare professional is concerned that a child or adult may be at risk of death or serious harm. Professionals who have such concerns should draw the individual to the attention of the relevant authorities

In the interest of the public:

- When there is a serious risk to public health

- When there is a risk of serious physical/mental harm to the individual or those known to the individual
- For the prevention, detection or prosecution of a serious crime
- Where disclosure is necessary to protect vital interests (i.e. where there is knowledge or belief of abuse or neglect of a child or adult at risk)
- Circumstances detailed in policy or guidance of the organisation where the care professional is working.
- Where the disclosure is otherwise lawful.
- If in doubt, seek the advice of the local SIRO or Data Protection Officer of the organisation (whether that is Florence or for care professionals on assignment, the organisation they are working within).

Refusal of consent

Service users have the right to object to the information they provide in confidence being disclosed to a third party in a form that identifies them, even if the third party is someone who might provide essential healthcare. Where service users 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 service user exercising their right to refuse treatment. A number of issues to be considered if a service user refuses to consent to information sharing are as follows:

- The concerns of the individual must be clearly established, and attempts should be made to find out whether there is a technical or procedural way of satisfying these concerns without unduly compromising care
- The options for providing an alternative form of care or to provide care through alternative arrangements may need to be explored
- Decisions about the options for alternative arrangements that might be offered to the service user have to balance the risks, employees time and other costs that may result against the risk to the individual of not providing assessment, care or treatment.

Careful documentation of the decision-making process and the choices made by the service user must be documented in the service user's records.

Rights of all Individuals

All Individuals may view personal information we hold about them. Local health authorities are not required to give access to information that is 'hurtful' or 'that would breach the confidentiality of another Individual'. The policy of Florence is to record information in a way that, as far as possible, avoids a need for this exclusion. If an Individual believes their right to confidentiality is either being breached or undermined, they must have access to the complaint's procedure at Florence.

Rights of all employees

All employees may view personal information held by Florence that relates to them, by applying in writing to their Line Manager or Registered Manager.

Anonymisation

Anonymised information (i.e. where personal information is removed and both the giver and the receiver are unable to identify the Individual) is not confidential and may be used outside of data protection legislation. However, employees should be aware that information which contains small numbers of person identifiable information may lead to identification. For this reason, all disclosure of anonymised information should be reviewed on a case-by-case basis. Florence will seek to anonymise collective data about individuals within Florence.

Pseudonymisation

Pseudonymisation is the practice of removing and replacing actual data with a coded reference (a 'key'). Florence will consider this practice where the use of the data needs to relate to individual records, but also needs to retain security and privacy for that Individual. There is a higher privacy risk and security risk of the key system as the data will not truly be anonymised.

Personal data that has been pseudonymised can fall within the scope of data protection legislation depending on how difficult it is to assign it to a particular individual.

Suppliers

Employees must extend the principles of confidentiality when considering Florence sensitive information and the protection of any commercial data.

Employees and/or external suppliers will ensure that information such as suppliers' prices, performance and costs are not disclosed to other suppliers or unauthorised persons. Florence could consider requesting that suppliers sign a confidentiality agreement in order to protect the data of Florence.

Meetings

Florence has a right to have confidential meetings where information is discussed and then held securely and confidentially. Information held will be in line with the Freedom of Information Act (FOIA) 2000 and UK GDPR, the Data Protection Act 2018.

Complaints and Investigations

Complaints and investigations are treated confidentially and remain so unless there is a legal requirement to release information.

Media

Employees must not pass on any information, or make comments, to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries.

Confidentiality Breach

Unauthorised access, use or disclosure may be in breach of the UK GDPR, DPA 2018, the Human Rights Act, and/or breach the policies of Florence and may lead to disciplinary action.

Where there has been a breach in confidentiality, this will be recorded on an incident form at Florence and reported.

Significant breaches will be reported to the Director of Quality and Governance so that reporting to the relevant regulatory, professional bodies and the ICO is considered.

Breaches will be monitored and reflected on with lessons learned and will form part of the quality assurance programme for Florence.

6. Monitoring and Compliance

Regular reviews of this policy will occur every three years or sooner in response to legislative, registration, or policy changes.

7. Policy Changes/Version History

Date	Reviewed changes
02/09/2024	Registered manager changed