Lindsey Lodge Hospice & Healthcare

CONFIDENTIALITY AND DATA PROTECTION POLICY

Contents

1 Introduction

Lindsey Lodge is a third sector, voluntary organisation and it is acknowledged whilst we are a non NHS organisation we will adopt the best practice and standards required of all employees working in the NHS, who are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. We will follow this because this is not just a contractual responsibility but also a requirement within:

- Common law duty of confidence
- Data Protection Act 2018
- NHS Care Record Guarantee

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non NHS organisations. It lays down the principles that must be observed by all staff within Lindsey Lodge to ensure they are aware of their responsibilities for safeguarding confidentiality, preserving information security and ensuring compliance with the Data Protection Act.

Lindsey Lodge needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, service users, employees (present, past and prospective), volunteers and suppliers. The information includes name, address, email address, data of birth, and private, confidential and sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current F4 IT and NHS Encryption Guidance.

Confidential information within a clinical setting is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, Gift Aid forms and Supporter/Donor Information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, tablets, mobile phones, digital cameras or even heard by word of mouth.

The lawful and proper treatment of personal information by Lindsey Lodge is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that Lindsey Lodge treats personal information lawfully and correctly.

A summary of Confidentiality Do's and Don'ts can be found at *Appendix A*.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in *Appendix B*.

How to report a breach of this policy and what should be reported can be found in *Appendix C*.
Definitions of confidential information can be found in *Appendix D*.

2 Scope

This policy applies to all staff working for or on behalf of Lindsey Lodge, including permanent staff, bank staff and Volunteers.

3 Roles and Responsibilities

3.1 Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that Lindsey Lodge policies comply with all legal, statutory and good practice guidance requirements.

3.2 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-and-service-user-identifiable information. The Medical Director holds this role within the hospice.

3.3 Data Protection Officer

Data protection officer is the first point of contact on all data protection matters. They are responsible for overseeing our data protection strategy and implementation to ensure compliance with the Data Protection Act. The Business Manager holds this position.

3.4 Workforce Team

The Workforce Team are responsible for ensuring that the contracts of all staff (permanent and temporary) reflect the contractual requirements of this policy and that confidentiality is included in corporate inductions for all staff **and to ensure all new** volunteers are made aware of the expectation around and their obligation to confidentiality via their induction training.

3.5 Information Governance Lead

The IG Lead is responsible for maintaining the currency of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application. The Business Manager is our IG lead.

3.6 Line Managers

Line Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted on by logging these on the incident process and following the incident policy.

3.7 All Staff including bank staff and volunteers

All individuals will, through appropriate training and responsible management:

- Participate in induction, training and awareness sessions carried out to inform and update staff on confidentiality and data protection issues.

- Observe all forms of guidance, codes of practice and procedures about confidentiality, data protection and the collection and use of personal information.

- Understand fully the purposes for which Lindsey Lodge uses personal information.

- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Lindsey Lodge to meet its service needs or legal requirements.

- Ensure the information is correctly input into Lindsey Lodge systems.

- Ensure the information is destroyed (in accordance with the provisions of the Data Protection Act) when it is no longer required.

- Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian.

- Understand that breaches of this Policy may result in disciplinary action, including dismissal or in the case of volunteers the withdrawal of the volunteering arrangements.

4 Confidentiality

4.1 Confidentiality Principles

All staff must ensure that the following principles are adhered to:-

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.

- Access to person-identifiable or confidential information must be on a need-to-know basis.

- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.

- Recipients of disclosed information must respect that it is given to them in confidence.

- If the decision is taken to disclose information, that decision must be justified and documented.

- Any concerns about disclosure must be discussed with either your Line Manager, Data Protection Officer or the Caldicott Guardian.

- Arrangements for the storage and disposal of all personal information (both manually recorded and computer based) must protect confidentiality and be in line with the Records Management retention recommendations.

Lindsey Lodge is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Access to rooms and offices where workstations are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular, they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked. Confidential waste bags should be stored out of sight in the office or locked away if possible.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bag, USBs and printouts must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality which individuals are required to complete on taking up appointment, or in the case of Volunteers a Statement of Confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal or in case of volunteers' withdrawal of the volunteering arrangements.

4.2 Disclosing Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised.

- If the patient withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made when the information is required by law or under a court order or can be justified in the public interest. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the NIGB Ethics and Confidentiality Advisory Group.

If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance staff.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance team.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries and e-mails. See the Information Security Policy for guidance on the safe transfer of confidential or person-identifiable information.

Transferring patient information by email to anyone outside NHS mail may only be undertaken by using encryption, since this ensures that mandatory government standards on encryption are met.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or contain confidential information and after agreement from the Data Protection Officer or Caldicott Guardian.

4.3 Duty of Care

All staff/volunteers have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.

- Leave any person-identifiable or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes and other documents.

- Leave a computer workstation logged on to a system where person-identifiable or confidential information can be accessed, unattended.

- Dispose of identifiable information in the confidential waste bag, ensuring that this is stored out of sight in an office or locked away where appropriate.

Steps must be taken to ensure physical safety and security of person- identifiable or business confidential information held in paper format and on computers.

Staff allocated a Systm 1 smartcard, should ensure they adhere to NHS smart card rules in relation to not leaving the card unattended or sharing of smart cards. Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff/Volunteers must not use someone else's password to gain access to information. Action of this kind may be considered as a serious breach of confidentiality or data security. This is potentially a disciplinary offence and could result in dismissal, or in the case of volunteers' withdrawal of the volunteering arrangements.

4.4 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate organisational purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act and may result in disciplinary action, or in the case of volunteers' withdrawal of the volunteering arrangements.

When dealing with person-identifiable or confidential information of any nature, individuals must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of Lindsey Lodge.

If individuals have concerns about this issue they should discuss it with their Line Manager, Data Protection Officer or the Caldicott Guardian/ Speaking out Guardian

4.5 Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by IT & IG Committee (a subgroup of the Finance & Business Development committee) through a programme of audits. Evidence will also be required for the Data Security and Protection Toolkit.

5 Data Protection

5.1 Data Protection Principles

Lindsey Lodge Hospice fully supports and complies with the eight principles of the 2018 Act which are summarised below:

1. Personal data shall be used fairly and lawfully.
2. Personal data shall be used for specified, explicit purposes
3. Personal data shall be used in a way that is adequate, relevant and limited to only what is necessary.
4. Personal data must be accurate and kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with rights of data subjects.
7. Personal data shall be handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss destruction or damage.

6 Associated Policies and documents

Information Governance Policy
Information Security Policy
Records Management Policy
Social Media Policy
Internet Use Policy
Email Use Policy
Disciplinary Policy
Volunteering Policy
Speaking out Policy

Appendix A: Confidentiality Dos and Don'ts

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of Lindsey Lodge

- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised. Make sure that the confidential waste bag is out of sight of locked away if able to be.

- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

- Do ensure that you cannot be overheard when discussing confidential matters. Try to have discussions in private.

- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

- Do share only the minimum information necessary.

- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality straight away.

- When divulging information over the telephone, identify the caller to ensure that you have the appropriate authority from the patient. Use a password where possible.

- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.

- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.

- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and NHS Mandated Frameworks

Lindsey Lodge is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to all employees including staff and volunteers agents of Lindsey Lodge, who may be held personally accountable for any breaches of information security for which they may be held responsible. Lindsey Lodge fully complies with the Data Protection Act 2018 as well as the following:

The Caldicott Report (1997) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.

Article 8 of the **Human Rights Act (1998)** refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The **Computer Misuse Act (1990)** makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

The **NHS Confidentiality Code of Practice (2003)** outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3
We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Commitment 9
We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix C: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported through the Lindsey Lodge Incident Management system, on the Incidents database held on our L drive. This must be reported to either the Data Protection Officer, Caldicott Guardian, IG Lead, Senior Information Reporting Officer (SIRO) or the Chief Executive straight away. The process of addressing the incident will be managed to ensure compliance with Data Protection. Significant issues will be subject to full investigation and reporting action. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with the Data Protection Officer Line Manager/Team leader or IG staff. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to Lindsey Lodge systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing of person-identifiable information in ordinary waste paper bin rather than the confidential waste bag.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of the Caldicott Guardian, Data Protection Officer or Line Manager should be sought straight away.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the IT & IG Committee. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. 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.

Sensitive personal information as defined by the Data Protection Act 2018 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

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

7 Consultation

IT & IG committee and Senior Managers

8 Dissemination

Via Lindsey Lodge `L` drive Policies/Guidelines of this form.

9 Equality Act

9.1 In accordance with the Equality Act (2010), the Hospice will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Hospice will endeavour to develop an environment within which individuals feel able to disclose any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

9.2 The Hospice will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010)

REFERENCES: Care Plus IT Group (LLH IT Provider), ICO website, Data Protection Act 2018				
Lead Author of Policy: Kay Fowler, IT Support Officer **Responsible Sub-group IT & IG Committee** **RATIFICATION DATE BY TRUSTEES 26/02/2019** Review interval 2 year				
TO BE REVIEWED	REVIEW COMPLETED	BY	APPROVED BY	CIRCULATION
July, 2018	Feb 2019	Kay Fowler	IT & IG Committee	All Staff –access via L Drive
Feb 2021	June 2021	Kay Fowler	IT & IG Committee	L: Policies & Guidelines
June 2023				