NORTH HERTS HOSPICE CARE ASSOCIATION

Data Security and Protection Policy

Approval

Date policy was formally approved: March 2019

Agreed by:

Signature of Chairman of Trustees:

Signature of Chief Executive: 

Type of change: Minor changes

Policy history:
2019: Content reviewed in line with the provisions of the Data Protection Act 2018 (including General Data Protection Regulations (GDPR)) and the requirements of the new Data Security and Protection Toolkit. Name changed from Information Governance Policy to Data Security and Protection Policy. 2017: Content reviewed; format updated from Version 0 Sept 2014.

Next review

Person responsible for next review: Sue Plummer: Senior Information Risk Owner, Data Protection Officer, Chief Executive

Committee responsible for next review: Data Security and Protection Committee
Next review date: March 2022

Policy Statement
Information is a vital asset and resource, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in the clinical governance, service planning and performance management of Garden House Hospice Care (GHHC).
Data Security and Protection is a set of principles, policies and procedures which allow organisations to manage information effectively. It covers personal information (i.e. that relating to patients, service users and employees) and corporate information (i.e. financial, fundraising and accounting records).
The aim of Data Security and Protection is to facilitate the secure use of information in accordance with law and in a way that maximises the benefit to patients and service users.
GHHC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
GHHC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. It is the responsibility of all Hospice Team Members to ensure and promote the use of quality information.

Contents

1. Policy Statement

Information is a vital asset and resource, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in the clinical governance, service planning and performance management of Garden House Hospice Care (GHHC).

Data Security and Protection is a set of principles, policies and procedures which allow organisations to manage information effectively. It covers personal information (i.e. that relating to patients, service users and employees) and corporate information (i.e. financial, fundraising and accounting records).

The aim of Data Security and Protection is to facilitate the secure use of information in accordance with law and in a way that maximises the benefit to patients and service users.

The operational standards that Data Security and Protection sets out empower an organisation to become consistent in the way it handles information. In doing so, the organisation can safeguard itself from any accidental or deliberate misuses of information.

The aims of GHHC with regard to Data Security and Protection are to:

- Hold information securely and confidentially
- Obtain information fairly and efficiently
- Use information effectively and ethically
- Record information accurately and reliably
- Share information appropriately and lawfully.

This policy applies to:

- All information used by the GHHC
- All information systems managed by GHHC
- Any individual using information "owned" by GHHC
- Any individual requiring access to information "owned" by GHHC.

GHHC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. GHHC fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients & staff and commercially sensitive information. GHHC also recognises the need to share patient information with other health organisations & other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

GHHC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. It is the responsibility of all Hospice Team Members (staff and volunteers) to ensure and promote the quality of information.

This Data Security and Protection Policy covers four key, interlinked, strands:

- Openness
- Legal compliance
- Information security
- Quality assurance.

2. Related Hospice Policies/Procedures/Guidelines – see Appendix 1

3. Responsibility/Accountability

It is the role of the Data Security and Protection Committee to define GHHC's policy in respect of Data Security and Protection (DS&P), taking into account legal and NHS requirements. The Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Chief Executive has ultimate responsibility and holds the role of Senior Information Risk Officer (SIRO). The SIRO is expected to understand how the strategic business goals of the organisaiton may be impacted by information risks. The SIRO is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Data Security and Protection. The key responsibilities of the SIRO include:

- Leading and fostering a culture that values, protects and uses information for the success of GHHC and benefit of its patients and service users
- Providing direction in formulating, establishing and promoting DS&P policies
- Ensuring that GHHC's approach to information handling is communicated to all staff and made available to the public
- Coordinating the activities of staff given data protection, confidentiality and Freedom of Information responsibilities
- Monitoring GHHC's information handling activities to ensure compliance with law and guidance
- Ensuring Hospice Team Members are sufficiently trained to support their roles
- Ensuring that GHHC submits its annual Data Security and Protection Toolkit Assessment
- Supporting monitoring visits from the commissioning organisation
- Raising awareness of DS&P and providing a focal point for the resolution and/or discussion of DS&P issues
- Owning GHHC's overall risk management processes and ensuring that they are implemented consistently.
- Owning GHHC's information risk and incident management framework
- Ensuring there are adequate arrangements in place for reporting DS&P incidents or near misses; analysing, investigating and upward reporting of incidents or near misses with recommendations for remedial action (in accordance with RM20)
- Ensuring that the annual assessment and improvement plans are prepared for approval by the Board of Trustees.

The Chief Executive is also the Data Protection Officer; responsible for ensuring that all sensitive personal information that GHHC holds is used appropriately with respect for confidentiality and privacy of individuals and in line with the provisions of the Data Protection Act 2018 (including General Data Protection Regulations (GDPR)).

The Chief Executive is the Freedom of Information Lead for GHHC; ensuring that GHHC fully complies with all aspects of the Freedom of Information Act 2000.

Within GHHC, the Medical Director performs the role of Caldicott Guardian. The Caldicott Guardian:

- Acts as the conscience of GHHC
- Provides a focal point for patient and service user confidentiality and information sharing issues
- Oversees the management of patient and service user information.

Managers and Team Leaders within GHHC are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. For example (this list is not exhaustive):

Role	Responsibility
Director of Human Resources and Volunteering	staff and volunteer information (e.g. Cascade, paper records)
Director of Finance	finance data (e.g. SAGE, paper records)
Director of Fundraising, Marketing and Communications	donor information (e.g. Donorflex, paper records, Gift Aid declarations, marketing information)

All staff (whether permanent, temporary or contracted), volunteers and contractors are responsible for being aware of their responsibilities in relation to DS&P and complying with related GHHC policies, procedures, guidelines and processes, on a day to day basis. This includes reporting any actual or near miss DS&P incidents.

All employees should be aware that breach of this policy could have serious consequences for GHHC either by causing loss or disruption to business or by resulting in a breach of legislation. Breaches will, therefore, be treated very seriously. Any departure from this policy without specific prior authority will be treated as misconduct and disciplinary action may be taken which could result in dismissal.

4. Openness

Non-confidential information on GHHC and its services should be available to the public through a variety of media, in line with GHHC's commitment to openness.

All staff are required to pass any Freedom of Information requests to the Chief Executive, or in her absence another member of the Hospice Senior Leadership Team, who will respond to requests in the appropriate manner.

Patients have ready access to information relating to their own health care, their options for treatment and their rights as patients.

GHHC has clear procedures and arrangements for liaison with the press and broadcasting media.

GHHC has clear procedures and arrangements for handling queries from patients and the public.

5. Legal Compliance

GHHC regards all identifiable personal information relating to patients, staff, volunteers (including Trustees) or donors as confidential except where national policy on accountability and openness requires otherwise.

GHHC has and maintains policies to ensure compliance with the Data Protection Act 2018 (including General Data Protection Regulations (GDPR)), Human Rights Act 1998 and the common law confidentiality.

GHHC has and maintains policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

6. Information Security

GHHC has and maintains policies for the effective and secure management of its information assets and resources.

GHHC promotes effective confidentiality and security practice to its staff and volunteers through policies, procedures and training.

GHHC has and maintains incident reporting procedures. All reported instances of actual or potential breaches of confidentiality and security are monitored and investigated. Where required, such breaches are reported to the Information Commissioner's Office (ICO) and / or Charity Commission and Duty of Candour requirements are met.

7. Information Quality Assurance

GHHC has and maintains policies and procedures for the effective management of patient and service user records.

Managers and Team Leaders within GHHC are expected to take ownership of, and seek to improve, the quality of information within their services.

Information quality is assured at the point of collection wherever possible.

GHHC promotes information quality and effective records management through policies, procedures, guidelines, manuals and training.

8. Policy Monitoring and Review

The policy will be reviewed, as a minimum, every three years.

Audit will be carried out in line with the requirements of the Data Security and Protection Toolkit.

9. Compliance with Statutory/Professional Requirements

Data Protection Act 2018
Freedom of Information Act 2000
Access to Health Records Act 1990
Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
Care Quality Commission (Registration) Regulations 2009

10. Staff Training Requirements

Training on Data Security and Protection is given to all new Hospice Team Members on induction.

Mandatory Data Security and Protection training is completed annually by all Hospice Team Members at a level appropriate to their role and responsibilities.

Employee attendance at training is recorded on individual records in the Human Resources Database (Cascade).

Volunteers are required to complete mandatory training workbooks which include a section on Data Security and Protection. Completion of the workbook is recorded on individual records in the Human Resources Database (Cascade). Frequency of completion is reviewed every three years.

All staff must read relevant policies and procedures and work within them. They are required to sign on appraisal that they are up to date with policies.

Appendix 1. Related Policies, Procedures and Guidelines

RM08	Safeguarding Children Policy
RM10	Safeguarding Adults at Risk Policy
RM19	Risk Management Policy
RM20	Incident Reporting and Management (including Serious Incidents Requiring Investigation)
OM08	Volunteer Management Policy
OM12	Confidentiality Policy and Procedures
OM13	Health Records Management Policy
OM24	Information for Patients Policy
OM27	Finance Policy
OM32	Data Protection Impact Assessment Policy
OM33	Information Technology Security Policy
OM34	Information Technology Network Security and Infrastructure Policy
OM35	Media, Communications and Social Media Policy
OM46	Smartcard Policy
CM14	Access to Health Records Policy
CM22	Being Open and Duty of Candour Policy
HR02	Recruitment, Selection, Induction & Probation (inc. Disclosure & Barring Service) Policy
HR05	Disciplinary, Grievance and Appeal Policy