Data Protection Policy

Document Type: (please tick)	Policy	☒	Procedure	☐
	Standard	☐	Guidance	☐
Postholder:	HR & OD Manager			
Version no:	3.0			
Final approval date:	11 October 2021			
Interested Groups / Boards/ Committees with whom this document is shared for initial feedback/comment:	Information Governance Group Quality and Governance			
Name of Final Approving Group, Board or Committee:	Executive Management Team			
Date for Review:	***October 2024***			
Note: All documents are to be reviewed on 3 yearly basis unless a change is required by legislation, NHS Policy including NICE Guidelines etc, CQC requirements, commissioning requirements, changes in professional practice evidenced by e.g. Codes of Practice developed by Professional Bodies, changes in the structure of the organisation, significant incident or adverse occurrence.				

Groups <u>to be notified</u> about this document: *Please detail staff/volunteer groups or roles who need to be notified the document has been published:*	The Information Governance Group			
Groups <u>affected by</u> this document: *Please detail staff/volunteer groups or roles to whom the policy/document is relevant:*	All staff and volunteers.			
Category *(to be applied when uploading to Sharepoint.*	Clinical	☐	Medicine Management	☐
	Corporate	☐	Health & Safety	☐
	Fundraising	☐	Human Resources	☐
	Information Governance	☒	COVID specific	☐
	Volunteer	☐		

Contents

1 Purpose of Policy

1.1 Pilgrims Hospices is a charity supporting people living in East Kent. Pilgrims Hospices needs to collect personal information (Data) about people we interact with in order to carry out our business and provide our services because:

- We provide healthcare and psychosocial services to our patients and their families and carers.
- We work with a range of external providers to ensure the provision of effective and joined-up care across a patient's care pathway.
- We ask for support from fundraisers and donors.
- We raise funds via our lottery.
- We approach trusts and grant makers for funding.
- We raise funds via our retail outlets.
- We actively fundraise in our local community.
- We provide training for healthcare professionals and organise education events for the East Kent community.
- We manage various functions, such as HR or payroll that require us to keep and share (personal) data about our staff and volunteers.

1.2 Therefore, people on whom we may hold data include but are not limited to; patients and their next of kin, employees (present, past and prospective), volunteers, supporters, suppliers, external professionals, other business contacts and members of the general public.

1.3 The information we might hold or process on individuals may include but is not limited to: name, address, email address, date of birth, private and confidential information, and sensitive information. We often hold financial or health data on individuals.

1.4 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 handled in compliance with the Data Protection Act 2018 (the Act) and General Data Protection Regulation 2018 (GDPR).

1.5 The lawful and proper treatment of personal information by Pilgrims Hospices is extremely important to our success and in order to maintain the confidence of our service users, supporters and employees. We ensure that we treat personal information lawfully and correctly.

1.6 This policy incorporates the principles of the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

1.7 For the purposes of this policy, personal data has the following definition:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

This definition covers written information, including records held physically and electronically, as well as images, video or audio recordings.

2 Responsibilities

2.1 Pilgrims Hospices is not required to appoint a Data Protection Officer, however, has taken the decision to instead appoint a Data Protection Lead.

- Ensure that there is always a designated individual with overall responsibility for data protection. This person is the IT Manager who is appropriately trained, experienced in data protection and is familiar with all of the relevant systems and processes in their day-to-day role.
- Provide appropriate training for all staff members and volunteers who handle personal information.
- Provide clear lines of report and supervision for compliance with data protection.
- Carry out regular checks to monitor and assess new processing of personal data and to ensure the Pilgrims Hospices notification to the Information Commissioner is updated to take account of any changes in processing of personal data.
- Develop and maintain Data Protection procedures to include: roles and responsibilities, notification, subject access, training and compliance testing.
- Conduct regular information audits to support compliance and ensure data is up-to-date and relevant.

2.2 Data Protection Lead: IT Manager.

- Responsible for the application of policy and procedure, provision of guidance, training and support for the implementation of Information Governance principles in all strategic and service developments and day to day provision of services and care.

- Monitoring and reporting on compliance to the Executive Directors.
- To report any breaches to appropriate external bodies, e.g. the Office of the Information Commissioner, as required.
- To ensure the principles of Data Protection and information governance are applied as part of normal practice in the provision of care and other services.

2.3 Caldicott Guardian: Director of Nursing and Care Services

- Responsible for the management of patient /service user confidentiality and information use, sharing and disclosure issues by:
  - Providing advice and being accountable for that advice.
  - Being the conscience of the organisation.
  - Providing a focal point for patient/service user confidentiality and information sharing issues.
  - Being concerned with the management of patient /service user information.

2.4 Senior Information Risk Owner: Director of Finance & ICT

- Take overall ownership of the Organisation's approach to information risk management and provide oversight of Information Governance risks.
- Ensure information risks are recorded and adequately mitigated.
- Provide advice to the EMT and Board regarding the management of information risks.

2.5 Information Asset Owners: Directors who are directly responsible for the databases and information related to their department:

- Patient Databases: Director of Nursing and Care Services
- Finance Databases: Director of Finance and ICT.
- HR and Payroll Database: Head of Workforce.
- Fundraising/Donor & Lottery Databases: Director of Income Generation.
- Retail Databases: Director of Income Generation.

2.6 Information Asset Administrators: – department managers who manage the use of the data.

2.7 Users: anyone processing data as part of their work (this includes accessing, collecting, recording, amending and disseminating data for any purpose).

2.8 All employees will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures

about the collection and use of personal information.
- Understand fully the purposes for which Pilgrims Hospices uses anypersonal information relevant to the employee's role.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Pilgrims Hospices to meet its service needs or legal requirements.
- Ensure the information is input into all Pilgrims Hospices systems.
- Ensure the information is securely destroyed when it is no longer required in accordance with .
- On receipt of a request for information held about a patient, immediately notify the Caldicott Guardian..
- 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.

3 Data Protection Principles

3.1 The Principles

All personal data obtained and held by the organisation will be processed in line with the data protection principles. These are summarised below:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure) ***[See Below]***
- the right to restrict the processing of the data
- the right to portability

- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.
- The right to lodge a complaint with a supervisory authority.

It should be noted that, while an individual may withdraw consent for their data to be processed and request deletion of this data, the organisation can only comply with the request to delete information where no conflicting obligation requires the organisation to retain this information i.e. legal requirements to retain employee or financial records for statutory retention periods.

3.2 Application

Pilgrims Hospices maintains a Record of Processing Activity (ROPA) which outlines our approach to the application of the data protection principles and activities we undertake to ensure our processing meets the reasonable expectations of the data subjects. The ROPA includes:

- The ***lawful basis*** for collecting and processing personal data including sensitive and special category personal data.
- The ***limited purpose*** for which the organisation processes data in line with our business objectives and the processing activities associate with each objective.
- Organisational processes to ensure ***minimisation of data*** in day-to-day operations.
- Organisational processes to ensure ***accuracy of data*** in day-to-day operations.
- Organisational processes for the ***storage and disposal*** of data and guidance regarding retention periods.
- Organisational processes to ensure ***integrity and confidentiality*** in day-to-day operations.

4 Access to Records (Subject Access Requests or 'SARs')

4.1 The relevant Director will take responsibility for any SARs relating to their area on behalf of Pilgrims Hospices. Where a request relates to data that falls within the purview of more than one Director, the request will be handled by the Director responsible for the area from which the majority of the data is requested.

4.2 Patients and anyone else on whom we hold records (staff, volunteers, donors, etc) have the right of access to their records or healthcare records in line with the requirements of the Data Protection Act 2018 and GDPR Regulation 2018.

4.3 Requests to access records must be made in writing and specify the data requested.

4.4 The Hospice will respond to any request within the legal timeframes.

4.5 The Hospice reserves the right to refuse a request or levy a charge for responding to SARs where requests are deemed to be manifestly unfounded, excessive, or in instances where the requested information has previously been provided.

4.6 In some cases where information recorded is assessed as detrimental to the health or well-being of the individual, information may be withheld. In the case of healthcare records, this must be justified and recorded appropriately by the relevant Directors.

4.7 Patient representatives may request copies of patient medical records. Such requests should be made in writing to the Director of Nursing and Care Services, who will liaise with the appropriate clinician prior to providing copies of notes made. The Hospice reserves the right to make a moderate charge for this service.

4.7.1 Patients or their representatives MUST NOT be given the original copy of their notes to take away – ownership lies with the Hospice.

4.8 Third Party Requests. In some cases, other third parties may request access to records, e.g., Police, Solicitors, Insurance Companies, etc. Requests should be made in writing to the Director of Nursing and Care Services, who will liaise with the Consultant, key clinician or appropriate manager prior to providing copies of any data.

Requests should be submitted in writing to:

Pilgrims Hospice Canterbury
56 London Road,
Canterbury,
CT2 8JA

4.9 This section should be read in conjunction with the Privacy Policy, Subject Access Request Policy and Request for Copy of Health Records Policy which can be found on both the external internet site and internal intranet.

5 Donor Data

5.1 Donor data will be processed in line with legislation and guidance, including, but not limited to the Data Protection Act, and guidance from the Fundraising Regulator's Code of Fundraising Practice available from their website: https://www.fundraisingregulator.org.uk/

5.2 We will use personal information:

- To provide services, products or information requested.
- To create an account for donors if registered with us.
- For administration purposes.
- To further our charitable aims, including our fundraising activities.

5.3 We may analyse and screen the personal information we collect to create a profile of donor interests and preferences so that we can contact donors in the most appropriate way and with the most relevant information. Where relevant, we may also assess donor personal information for the purposes of fraud prevention.

5.4 We work in line with the General Data Protection Regulation which came into effect from May 2018. We will contact potential donors based upon their expressed preferences for contact from us.

5.5 Under the GDPR there are different legal conditions through which we can send direct mail to an individual. One of them is called 'legitimate interest'. This enables us, in certain circumstances, to send direct mail to an individual where we believe there to be a genuine interest in receiving the information, i.e. where we invite next-of-kin to our remembrance events. When we mail through legitimate interest we will always make sure that individuals have the opportunity to say 'no' or object to future direct mail.

5.6 Under both the current data protection rules, and the GDPR, we will send direct marketing by post where:

- There is a legitimate interest, *AND*
- The legitimate interest is not overridden by the rights and interests of the individual.

5.7 Our donors and supporters will be treated fairly and respectfully and we will ensure that we meet our legal obligations.

5.8 We will undertake a balancing assessment to consider what an individual would reasonably have expected their personal information to be used for at the time that they provided it.

5.9 We publish privacy notices which go into more detail about how we do this.

5.10 Keeping donor data safe - Personal information and details of enquiries received are stored on a secure database.

5.11 If for any reason a donor wishes to have personal details removed from our records, they can contact us and request that data is removed. We will

delete data we no longer need and are no longer required to retain.

Where records include financial transactions we may have a legitimate reason to retain the information due to HMRC, auditing guidelines, regulatory and legal requirements. On these occasions we will mark your records to ensure your receive no further contact from Pilgrims
If your request to delete personal information is due to wanting no future contact from Pilgrims, please note that the best way to guarantee no further contact is for Pilgrims to retain your record and mark accordingly. Once we delete your information we will retain no record of your request for no future contact.

5.12 We will not actively contact anyone who has not actively supported us in the last 8 years.

6 Training

6.1 New employees must read and understand the policies on data protection as part of their induction.

6.2 All employees receive training covering confidentiality, data protection and the actions to take upon identifying a potential data breach.

6.3 The nominated data controllers for the organisation are trained appropriately in their roles under GDPR and DPA 2018.

6.4 All employees and volunteers who need to use the computer system are trained to protect individuals' private data, to ensure data security and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company policies and procedures

7 Monitoring

7.1 Compliance with the policies and procedures laid down in this document will be monitored by the Information Governance Committee, together with independent reviews by auditors.

8 National Data Opt-Out

8.1 As a health care organisation in England, from 30th September 2021 Pilgrims Hospices has been subject to the national data opt-out policy. We do this through the national data opt out service that allows patients to opt out of their confidential patient information being used for purposes other than direct patient care. National data opt out applies in situations where it is not practical for informed consent to be sought from a patient for their

clinical record data to be used for purposes such as research, planning, service evaluation, service improvement or national audit. The national data opt-out does not cover data disclosures that we are required to make by law. Nor does it cover local audit as this is considered to be direct patient care.

The national data opt-out policy should be considered and assessed when handling any new disclosure request for data processing which could potentially be used for purposes other than direct patient care. Any data disclosure request or data processing deemed to be covered by national data opt out should be requested through Pilgrims Hospice Database/Business Intelligence Manager, or they should be informed before any data processing takes place. They will then be able to review the dataset for patients who have opted out of their data to be used, and they will remove these patients from the dataset before the data is processed.

To be compliant Pilgrims Hospices are obligated to communicate with our service users that we may use their data for purposes other than their direct patient care and inform them of how they may opt out e.g. through posters, leaflets and privacy notice.

Staff should refer to Pilgrims Hospices' guidance document: ***'National patient data opt out'*** which is available via sharepoint for further information on identifying what data/when the national data opt-out applies; the process for staff to follow if they are processing or requesting data covered by national data opt out; what staff should do if a patient in our care wishes to opt out.

9 Compliance

9.1 Any deviation in practice or failure to comply with this policy will be deemed a breach of policy. Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the organisation becoming aware of it. Where it is not possible to complete a full report within 72 hours, an initial report may be made with a view to following up and providing additional information.

9.2 Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

9.3 If the breach is sufficient to warrant notification to the public, the organisation will do so without undue delay.

9.4 Any breach of this policy by Pilgrims Hospices employees may lead to formal disciplinary action.

9.5 Any breach of this policy by Pilgrims Hospices volunteers may lead to formal action under the Problem Solving Policy and Procedure.

All employees retain the right to discuss the contents of this document with management at any time.

Document History			
Version	**Publication Date**	**Author / Editor**	**Summary of Change**
1.0	22/02/2018	Human Resources	Publication
2.0	18/02/2020	Human Resources	Updated format and minor amendments
3.0	11/10/2021	Human Resources	Inclusion of National Data Opt-Out Information