Keeping confidential & personal information safe

General Data Protection Regulations

Guidance for Volunteers

Information Governance – Your Responsibility

Individuals entrust St Elizabeth Hospice to gather Person Identifiable Data (PID) about their clinical and personal situation. PID is any information with can identify certain individuals.

Individuals rightly expect that all persons who are exposed to and handle this information will use it appropriately and in line with the law.

The law is changing!

The Data Protection Act 1998 (DPA) is being replaced with the General Data Protection Regulations 2018 (GDPR) on 25 May 2018

- Like the DPA, the GDPR applies to 'personal data'
- However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. An IP address – can be personal data.
- The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – e.g. Key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. (for example MRS A B is clearly Mrs Anne Barrett)
- Under the GDPR, the data protection principles set out the main responsibilities for an organisation. The principles are similar to those in the DPA, with added detail at certain points and a new accountability requirement.

The most significant addition is the accountability principle. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about processing activity.

It is important that you determine your lawful basis for processing personal data and document this.

- Parental consent must be gained before personal data is held on anyone under 16.
- Additional consent must be gained for anyone with recognised mental capacity issues.

Individual rights under GDPR

1. The right to be informed – our obligation to provide fair processing information, typically through a privacy notice. It emphasises the need for transparency over how we use personal data
2. The right of access – to records held on or about them
3. The right to rectification – to have records corrected
4. The right to erasure – to have records deleted
5. The right to restrict processing – individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future.
6. The right to data portability – allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
7. The right to object to – processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) – direct marketing (including profiling) –and processing for purposes of scientific/historical research and statistics.
8. Rights in relation to automated decision making and profiling – GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Consent

Consent under the GDPR must be a freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions

Subject access rights

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of how their records are kept and managed.

We have 30 days to respond. All subject access requests are dealt with by the Data Protection Officer who processes the request. It is important that you inform them as soon as possible. Do not pass the information over to the individual.

Breach

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

A breach is more than just losing personal data, loss, destruction of, alteration, unauthorised disclosure or access to personal data, are all breaches.

If you think that we have had a data breach you MUST inform the Data Protection Officer immediately.

Disclosing Confidential Information

- Never discuss confidential and sensitive data or PID in public areas including corridors, lifts, on public transport or other communal space.
- Be aware of who can overhear your conversation. For example; if you work at a reception desk, ask the individual to state their own details to ensure you do not accidently read out the details of another individual
- Never discuss personal data with friends and family, including outside of work.

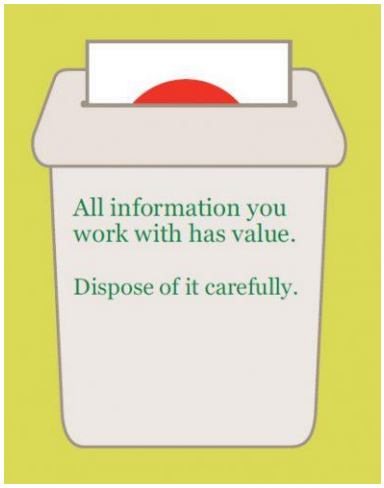
Keeping Data Safe

- Never share passwords to systems with anyone, always operate a clear desk policy and lock your computer whenever you are away from your desk.
- Think about who has access to the data that you hold, is the access appropriate, and how easy is it for an unauthorised person to access it?
- Be prepared to challenge people entering your work area; do you recognise them or do they have their ID badge displayed?
- When transporting confidential and sensitive data by hand, ensure it is secure, so that no data can be seen or lost.

- If transporting data or equipment (e.g. laptop) by car, place it in the boot of the car and ensure the car is locked. Do not leave it there for long periods of time, such as overnight.
- No PID should be emailed to your personal email address, and under no circumstances should information be saved to any personal IT devices. Never take patients, customers or staff records home with you unless you have been authorised to do so.

Destruction of Data

When printed or electronic copies of confidential and sensitive data or PID are no longer required, they should be destroyed in a manner approved by the Information Governance Lead.



Passing on PID – Important Issues to Remember

Email

If you need to email personal information to an external email address outside of the hospice; **Never** include a name within the email, and do not include personal identification details within the content of the email.

Post

When posting PID, ensure that it is sent in a sealed envelope contained within another robust sealed envelope bearing the address of the recipient. If data is extremely sensitive, ensure it is double wrapped and sent recorded delivery or by a courier.

Telephone

Never disclose PID over the telephone unless you are absolutely certain that you are speaking to the intended person. If using a mobile telephone, PID should never be shared via a text message.

Answer Phones/Voicemail

Only leave messages on answering systems if the recipient has consented or you are confident that only the intended recipient will receive the message.

Laptops and Memory Sticks

Only encrypted laptops or encrypted memory sticks supplied and approved by the hospice can be used for transporting PID in an electronic form.

Social Networking

The rule of confidentiality still applies when using social networking websites such as Facebook and Twitter.

You must not release any information on social networking sites which you have obtained as part of your job role

You must not discuss any aspect of patient care on social networking sites, even if you believe you are chatting to the actual patient

Defamatory remarks about the hospice or any of its staff and volunteers must not be made.

Please be aware that even though your public social networking content may be concerned with your private life, what's written may be subject to disciplinary action where it breaks your terms of employment or associated rules.

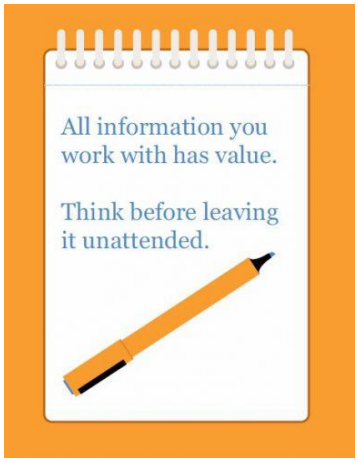
Remember!

Clear Screen Policy

Do not leave PID visible on unattended PC's. If you leave your desk, press CTRL+Alt+Delete to lock your computer and protect other data you are displaying.

Clear Desk Policy

Any papers containing confidential information must be placed out of sight, in locked cabinets or locked offices when not in use.



Clear Printer/Photocopier Policy

Ensure that PID is collected promptly from printers and photocopiers

Clear Drive Policy

Consistent with hospice IT procedures, NO data, confidential or not, is to be stored on the desktop of a computer

Hospice IT Procedures

Please refer to the 'Standard for the use of computing and telecommunications systems' available on HOLI, or ask you link/line manager for a copy

For full information please refer to the hospice GDPR policy available on HOLI, or ask your link/line manager for a copy.