Individual Rights and Data Access Procedure

Ensuring data subjects rights, and rights of access to data, are understood

Nick Banister-Dudley, Head of Compliance and Data Protection Officer

hallmark care homes

SANTHEM RESIDENCES

SANTHEM CARE

Policy number	HCH/NBD/OPS/68
Version number	2.0
Date of issue	20/07/2021
Date for review	19/07/2024
Author	Head of Compliance and Data Protection Officer
Ratified	Care Quality, Governance and Compliance Director and Senior Information Risk Owner
Outcome	Data subjects/individuals will be aware of their rights under the GDPR and other relevant legislation. The Hallmark Care Homes group of companies will be able to respond effectively and in a timely manner to any data access requests ensuring that people can access data in line with legislation.
References	• *The General Data Protection Regulation* • *Data Protection Act 2018* • *Access to Health Records Act 1990* • *Freedom of Information Act 2000* • *Information about the deceased (Information Commissioner's Office, version 1.1)* • *Guide to freedom of information (Information Commissioner's Office, accessed 11/01/2021)* • *Guidance for Access to Health Records Requests (Department of Health, February 2010)* • *Access to health records (British Medical Association, 2019)* • *Guide to the General Data Protection Regulation (GDPR) (Information Commissioner's Office, accessed 11/01/2021)* • *Outsourcing and freedom of information - guidance document (Information Commissioner's Office, version 1.3)*

If you have any comments or suggestions on this procedure document, please email: dpo@hallmarkcarehomes.co.uk

Contents

Equality and Diversity Statement

Hallmark Care Homes, Santhem Residences and Santhem Care is committed to the fair treatment of all regardless of age, colour, disability, ethnicity, gender, nationality, race, religious or spiritual beliefs, and responsibility for dependents, sexual orientation, or any other personal characteristic.

Hallmark's Vision

To be recognised as the leading provider of high quality, relationship-centred care for all residents.

Santhem Residences' Vision

To provide exceptional environments creating peace of mind, a life of freedom & discovery at a time that is right for all.

1. INTRODUCTION

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force, across the EU and applies to the UK.

One of the key changes brought about by the GDPR which businesses must be aware of, is how individuals' rights in respect of their personal data have been affected. The GDPR gives individuals (whether these be customers, contractors or team members) more control over the ways in which businesses process their personal data, and this has led to the granting of new rights for these individuals, as well as enhancing and improving rights that existed under the outgoing Data Protection Act 1998 and in the new Data Protection Act 2018.

This procedure provides individuals with information on their rights under the GDPR (and other legislation) and details our processes with regards to responding to such requests.

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

2. DEFINITIONS

Access to Health Records Act 1990 (AHRA): The AHRA is legislation that gives specific people access to the health records of a resident/client who has sadly passed away. More information is included in section 5.3 below.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all team members, contractors, agency workers, consultants, directors, and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all personal data relating to team members and personal data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Protection Officer (DPO): this term means an individual or entities whose role it is to assist the controller, to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO for Hallmark Care Homes, Santhem Residences and Santhem Care is Nick Banister-Dudley, Head of Compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein, and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Freedom of Information Act 2000 (FOIA): The Freedom of Information Act (FOIA) 2000 gives members of the public the right to request information from public authorities. More information is included in section 5.2 below.

Lawful basis: The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever a data controller processes personal data.

Other legislation: This term refers to both the Access to Health Records Act 1990 (AHRA) and the Freedom of Information Act 2000 (FOIA).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to data subjects when we collect information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, team privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data

including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: the General Data Protection Regulation ((EU) 2016/679) is legislation of the European Union that makes personal data subject to the legal safeguards specified in the GDPR. At the end of the UK-EU transition period, the General Data Protection Regulation (GDPR) forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (EUWA) (retained EU law). Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (DP Brexit Regulations) amends the retained EU law version of the GDPR. Schedule 2 amends the Data Protection Act 2018 (DPA 2018), including that it replaces the definition of the "GDPR" in the DPA 2018 with a definition of the "UK GDPR".

3. PURPOSE OF THE POLICY

This document details individual and data access rights under the GDPR (and other legislation), and the procedure for handling requests in relation to these rights.

This policy must be read in conjunction with the relevant Privacy Notices (found on the relevant organisation's websites).

4. SCOPE OF THE POLICY

The content of this policy will apply across the entire Hallmark Care Homes Group. This includes all Hallmark care homes, the Hallmark Care Homes Central Support office, Santhem Residences and Santhem Care. Where the terms 'organisation' or 'company' are used throughout this policy, they should be read to include all the companies or business areas mentioned in this section.

All team members across the organisation will be required to act in accordance with the contents of this policy.

5. SPECIFIC DETAILS

Data subjects (and other individuals) have a number of rights in relation to the personal information we process, as well as other data. These rights are enshrined in 3 main pieces of legislation, more detail on which, is provided in the subsequent sections.

Support will be given to those individuals requesting information and their request will be responded to under the appropriate legislation, even if they do not identify this themselves.

5.1 Rights under the GDPR

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

These rights are explained in more detail in the subsequent subsections.

5.1.1 The right to be informed

Articles 13 and 14 of the GDPR specify what data subjects have the right to be informed about. Data subjects have the right to be informed about the collection and use of their personal data. This information must include:

- The name and contact details of our organisation.
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to data subjects in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether data subjects are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

The information must be concise, transparent, intelligible, and easily accessible. We have

privacy notices for current and prospective team members and for residents/clients, relatives, suppliers, website visitors and enquirers. These privacy notices are available at the following locations:

	Hallmark Care Homes	Santhem Residences	Santhem Care
Current team members	E-learning portal (Elfy)	E-learning portal (Elfy)	E-learning portal (Elfy)
Prospective team members	Website	Website	Website
Residents/clients, relatives, suppliers, website visitors and enquirers	Website	Website	Website

All privacy information will be reviewed annually, or sooner should there be a change to the way in which the data is processed. If we plan to use personal data for a new purpose, we will update our privacy information and will make this available to data subjects, before starting any new processing.

Privacy information can also be provided via just in time notices, such as those on our website asking for consent for the use of cookies.

5.1.2 The right of access

Article 15 of the GDPR states that the data subject shall have the right to obtain from the controller, confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information. This request is known as a subject access request (SAR).

Subject access requests can be made by someone else, other than the data subject, providing they have authority to act. This could be in the form of a Power of Attorney or signed letter of authority (in respect of professional support services such as solicitors or advocates).

5.1.3 The right to rectification

Under Article 16 of the GDPR data subjects have the right to have inaccurate personal data rectified. A data subject may also be able to have incomplete personal data completed, although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

5.1.4 The right to erasure or the right to be forgotten

Under Article 17 of the GDPR data subjects have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

However, processes must be in place to erase the data where erasure applies Data subjects have the right for their data to be erased where:

- The personal data is no longer necessary in relation to the purpose for which it was collected/processed.
- The data subject withdraws their consent or objects to the processing and there is no

overriding legitimate interest to continue processing.

- The personal data was unlawfully processed or has to be erased in order to comply with a legal obligation.
- Data does not have to be erased where it is processed:
  - to exercise a right of freedom of expression and information,
  - to comply with a legal obligation or for the performance of a task of public interest,
  - for the exercise or defence of legal claims, or
  - for purposes relating to public health, archiving in the public interest, scientific/historic research, or statistics.

If data has been disclosed to third parties, then they will be informed about the erasure of the personal data.

5.1.5 The right to restrict processing

Article 18 of the GDPR gives data subjects the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. Data subjects have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. In most cases, data will not have to be restricted indefinitely, but the restriction may need to be in place for a certain period of time. During this time, we cannot process the restricted data in any way except to store it.

Data subjects have the right to restrict the processing of personal data where:

- They have contested its accuracy.
- They have objected to the processing and we are considering whether we have a legitimate ground which overrides this.
- The processing is unlawful.
- We no longer need the data, but the data subject requires it to establish, exercise or defend a legal claim.

We must inform the data subject before we lift the restriction.

If data has been disclosed to third parties, then they will be informed about the restriction on the processing of the data.

5.1.6 The right to data portability

Article 20 of the GDPR gives data subjects the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format. This right then allows data subjects to have this data transmitted to another controller or themselves, without hindrance from the controller to which the personal data have been provided.

The personal data must be provided in a structured, commonly used, and machine-readable form (e.g., CSV files).

If the individual requests it, we may be required to transmit the data directly to another

organisation, if this is technically feasible.

5.1.7 The right to object

Article 21 of the GDPR gives data subjects the right to object to the processing of their personal data. This effectively allows data subjects to ask us to stop processing their personal data. Data subjects have the right to object to:

- processing based on legitimate interests, the performance of a task in the public interest or the exercise of official authority (including profiling),
- direct marketing (including profiling), and
- processing for scientific/historic research or statistics.

Where the data subject objects to direct marketing we must act immediately. There are no exemptions or grounds to refuse.

Where a data subject otherwise objects to processing their personal data, then we must comply with this request unless we can demonstrate overriding compelling legitimate grounds to continue processing, or that the processing is for the establishment, exercise or defence of legal claims.

5.1.8 Rights relating to automated decision making and profiling

Article 22(1) of the GDPR gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling. Data subjects have the right not to be subject to a decision when:

- it is based on automated processing, and
- it produces a legal effect or a similarly significant effect on the individual.

We must ensure data subjects are able to:

- obtain human intervention,
- express their point of view, and
- obtain an explanation of the decision and challenge it.

'Profiling' is any form of automated processing intended to evaluate certain personal aspects of a data subject, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour, and location.

The above right does not apply if the automated decision:

- is necessary for entering into or performance of a contract between us and the data subject,
- is authorised by law (e.g., for the purposes of fraud or tax evasion prevention),
- is based on explicit consent, or
- does not have a legal or similarly significant effect on the data subject.

When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place, such as:

- Being fair and transparent about the logic involved.
- Using appropriate mathematical/statistical procedures.

- Implementing appropriate technical and organisational measures to correct inaccuracies and minimise the risk of errors.
- Keeping personal data secure in a proportionate way.

It is best to avoid making automated decisions based on sensitive personal data unless we have the explicit consent of the data subject or have reasons of substantial public interest.

5.1.9 Requests made under the GDPR

Requests made by data subjects to invoke any of these rights, can be made verbally or in writing.

The Data Protection Officer (DPO) has the responsibility for reviewing and responding to all requests made under the provisions of the GDPR. All requests will be acknowledged within 2 business days of receipt.

We may need to confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity. However, we will only request information that is necessary to confirm who the data subject is.

We can refuse to comply with a request if it is manifestly unfounded, or excessive. A request may be manifestly unfounded if:

- The data subject clearly has no intention to exercise their rights.
- The request is malicious in intent and is being used to harass the organisation with no real purposes other than to cause disruption.
- The request makes unsubstantiated accusations against the organisation or specific team members.
- The data subject is targeting a particular employee against whom they have some personal grudge.
- The data subject systematically sends different requests as part of a campaign, with the intention of causing disruption.

A request may be excessive if it repeats the substance of previous requests, and a reasonable interval has not elapsed, or it overlaps with other requests. However, it depends on the particular circumstances. It will not necessarily be excessive just because a large amount of information has been requested.

If we are not going to respond to the request, we will inform the data subject of the reason(s) for not taking action and of the possibility of them lodging a complaint with the ICO.

Subject access requests (SAR)

We shall , unless there is an exemption (see section 5.1.10 below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form). This will be provided within one month of receipt of the request. If the request is complex, or there are a number of

requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if it contains the personal data of other data subjects. If it does, we may redact the personal data of those other data subjects, prior to providing the data subject with their personal data.

If personal data of the data subject is being processed, we will provide the data subject with the data and the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

a) the purposes of the processing,
b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity),
c) if relevant, the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients overseas,
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing,
f) the right to lodge a complaint with the Information Commissioner's Office (ICO),
g) where the personal data are not collected from the data subject, any available information as to their source,
h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject, and
i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

<u>Requests relating to other rights of data subjects</u>

Requests relating to the other rights of data subjects will be assessed in line with statutory provisions. A formal response to the request will be made within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay. If we are able to fulfil the request, necessary steps must be taken to do so.

When responding to a request, the data subject will be informed of their right to lodge a complaint with the Information Commissioner's Office, if they remain dissatisfied.

We shall also communicate with third parties when we have upheld a data subjects request to invoke one of their rights relating to their personal data. For example, our third-party service providers who process the data on our behalf, unless this is impossible or involves

disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

5.1.10 Exemptions

There are a number of exemptions that exist in relation to the rights of data subjects. These are included in Schedules 2 to 4 of the Data Protection Act (DPA) 2018. The exemptions in the DPA 2018 may mean that we do not have obligations relating to some requests under the rights enshrined in the GDPR.

We will only consider whether we can rely on an exemption, on a case by case basis. Where appropriate, we will carefully consider the extent to which the relevant GDPR requirements would be likely to prevent, seriously impair, or prejudice the achievement of our processing purposes.

5.2 Rights under the Freedom of Information Act 2000

The Freedom of Information Act (FOIA) 2000 gives members of the public the right to request information from public authorities. Whilst the Hallmark Care Homes Group is a private company, the Freedom of Information Act applies to us in respect of duties we undertake on behalf of a public authority. We undertake duties on behalf of a public authority in the following ways:

- When we care for residents/clients in receipt of continuing healthcare (CHC) funding, on behalf of the NHS.
- When we care for residents/clients who are publicly funded, by a local authority.

Anyone, including those who are otherwise unconnected to the organisation, can make a request under the FOIA. Requests must be made in writing.

As such, unless an exemption applies (as stated in Part II of the FOIA), we would be required to respond to a request under the FOIA in respect of the information held or processed in relation to the public duties we undertake only.

5.2.1 Requests made under the FOIA

Under guidance issued by the Information Commissioner's Office, public authorities have the responsibility for replying to FOIA requests. Depending on the scope and context of the request, the DPO will determine the public authorities it applies to and send a copy of the request to them to respond to.

Requests will be acknowledged within 2 working days of receipt. Requestors will be informed of the public authorities that the request has been sent to.

The DPO will then oversee the relevant data being collated, so that this can be shared with the public authority in order for them to respond to the request.

5.3 Rights under the Access to Health Records Act 1990

The GDPR does not apply to the data of residents/clients who have sadly passed away. The Access to Health Records Act (AHRA) 1990 gives a right of access to health records of deceased resident/client to:

1. Personal representatives of the deceased: a personal representative is the executor or administrator of the deceased person's estate. Personal representatives have an unqualified right of access and do not need to give a reason for applying for access.
2. To persons who may have a claim arising out of the death of the individual. There is less clarity regarding the individuals and types of claim that this term applies to. As such, the DPO will make a determination whether to release records or not, based on the individual circumstances of the request.

5.3.1 Requests made under the AHRA

Requests made under the AHRA will be responded to by the DPO. Upon receipt of a request under the AHRA, the DPO will check the requestor meets the criteria in the Act, namely:

- Personal representative – evidence that the requestor is an Executor or Administrator of the deceased person's estate e.g. via a Grant of Probate.
- Claim arising out of the death – details on the potential claim should be sought from the requestor to determine whether this meets this criterion.

Requests will be acknowledged within 2 working days of receipt. Where the request concerns records that were made in the 40-days preceding the date of the request, a response (and the records, if applicable) will be given within 21 days. Where the request concerns information, all of which was recorded more than 40 days before the date of the request, a response (and the records, if applicable) will be given within 40 days.