CCTV and surveillance policy

Ensuring that surveillance technology is used in line with the requirements of the UK GDPR

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

hallmark care homes

SANTHEM RESIDENCES

SANTHEM CARE

Policy number	ALL/NBD/OPS/53
Version number	3
Date of issue	06/09/2023
Date for review	05/09/2026
Author	Head of Compliance and Data Protection Officer
Ratified	Care Quality, Governance and Compliance Director and Senior Information Risk Owner
Outcome	That CCTV and other permitted surveillance technologies are used appropriately, in line with legislation and in such a way that has a minimal privacy impact on individuals.
Cross reference	• Individual Rights and Data Access policy • Individual Rights and Data Access procedure • Data and IT security • Data protection/GDPR policy • Investigation policy • Feedback policy • Feedback procedure • Mental capacity/DoLS policy • Personal data breach policy
References	• *The UK General Data Protection Regulation* • *Data Protection Act 2018* • *Guide to the UK General Data Protection Regulation (UK GDPR) (Information Commissioner's Office, accessed September 2023)* • *Surveillance Camera Code of Practice (Biometrics and Surveillance Camera Commissioner, accessed September 2023)* • *CCTV and video surveillance guidance (Information Commissioner's Office, accessed September 2023)* • *Using surveillance in your care service (Care Quality Commission, accessed September 2023)*

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, 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

This policy details the requirements in respect of CCTV and other forms of surveillance under the UK GDPR. Protecting the confidentiality and integrity of CCTV images is a critical responsibility that we take seriously at all times.

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations.

The organisation is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

2. DEFINITIONS

CCTV: Closed-circuit television (CCTV) it the use of video cameras to capture and record live images of a surveillance location.

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 UK 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.

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 Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of 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.

Information Commissioner's Office (ICO): The ICO is the UK's independent body set up to uphold information rights. The ICO has both responsibility for ensuring the UK GDPR (and other legislation/regulations) are upheld, as well as responding to concerns from data subjects.

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.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity, or availability of personal data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of personal data is a personal data breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

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.

Related Policies: policies, operating procedures or processes related to this policy and designed to protect personal data. See page 2 of this policy.

Smart devices: A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols (such as Bluetooth, Wi-Fi or 5G) that can operate, to some extent interactively and autonomously. Some types of smart devices are smartphones, laptops, tablets, smart speakers and smartwatches.

Special category 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 policy sets out how the Hallmark Care Homes Group handles CCTV images and how CCTV and surveillance is managed throughout the organisation.

4. DUTIES

The Executive Leadership Team (ELT) are ultimately responsible for ensuring all team members comply with this policy and understand the need to implement appropriate practices, processes, controls, and training to ensure that compliance with the requirements of the UK GDPR is achieved and maintained.

Each General Manager (or equivalent) is responsible for implementing this policy within their home/location, ensuring they understand the content of the policy, for attending relevant training and for ensuring their team members attend/complete training commensurate to their role.

The Head of Learning and Development is responsible for ensuring team members receive training commensurate to their role so that compliance with the requirements of the UK GDPR can be assured.

The Regional Operations support team i.e., Operations Director, Regional Director, Regional Business Development Manager and Regional Care Specialist are responsible for ensuring their own understanding of this policy and ensuring appropriate escalation of queries and concerns to the Data Protection Officer (DPO).

The DPO is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. The DPO (or their nominee) will also conduct the annual CCTV audit in each business area. That post is held by Hallmark's Head of Compliance.

Please contact the DPO with any questions about the operation of this policy or about the requirements of the UK GDPR or if you have any concerns that this policy is not being, or has not been, followed.

5. SCOPE OF THE POLICY

The content of this policy will apply across the entire Hallmark Care Homes Group. This includes all Hallmark care homes, 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.

This policy does not apply to the Hallmark Central Support Office as Hallmark is not responsible for the CCTV that is in place in this location.

This policy must be used in conjunction with the other data protection policies. These are highlighted in the cross references section of this policy on page 2.

6. SPECIFIC DETAILS

6.1 Implementation/ongoing review of CCTV systems (data protection by design and default)

Under the Surveillance Camera Code of Practice, as issued by the Biometrics and Surveillance Camera Commissioner, CCTV operators should adopt the following 12 guiding principles. Adherence to this policy will ensure these principles are adopted.

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Data protection by design is an approach that ensures organisations consider privacy and data

protection issues at the design phase and throughout the lifecycle of any system, service, product, or process. Data protection by default requires organisations to ensure that they only process the data that is necessary to achieve their specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

The use of CCTV intrudes on the privacy of data subjects. Best practice guidance states that CCTV should only be used for a specific purpose and to address a specific issue. During the implementation or review of a CCTV system, the following factors should be considered prior to the installation:

1. The nature of the problem we are seeking to address and whether CCTV addresses that problem.
2. Whether CCTV is a justified and effective solution.
3. Whether other, less intrusive systems exist.
4. What effect the use of CCTV may have on individuals and how we will continue to uphold their rights.
5. Whether, considering the responses to points 1 to 4, the use of CCTV is a proportionate response.

A data privacy impact assessment should be completed, or a current one reviewed, prior to the installation of any new CCTV system. The Hallmark Data Protection Officer can assist with the completion of this.

6.2 Selecting and siting surveillance systems

The images collected by a surveillance system must be adequate for the purpose of crime prevention and safety. The type of surveillance system chosen and the location it operates within, must also achieve this purpose.

Any surveillance systems should allow us to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third-party data.

Both permanent and movable cameras should be sited and, image capture restricted, to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as property or premises not owned or managed by a Hallmark Care Homes Group company. The cameras must be sited, and the system must have the necessary technical specification, to ensure that unnecessary images are not viewed or recorded, and those images that are recorded, are of the appropriate quality.

CCTV cameras should only cover external areas such as grounds, car parks and access areas and internal areas such as entrance/reception areas or foyers.

6.3 Ensuring effective administration

The Hallmark Care Homes Group have CCTV for the purposes of crime prevention and safety. This purpose is stated in the relevant Privacy notices (available from the relevant company

website). The use of CCTV and the images captured should not be used for any other purpose. Those managing CCTV should do so in line with this policy.

Only the General Manager (or equivalent), regional operations team, Estates Manager, Deputy Estates Manager, and the Data Protection Officer should have the password for the CCTV system in each home. A General Manager (or equivalent) may choose to share the CCTV password with another Head of Department in their business area, so that CCTV can be accessed and managed in their absence, in line with this policy. The CCTV system should only be accessed in the actual business area, and not remotely or off site. Accessing CCTV images from any other location, is not congruent with the defined purpose that we use CCTV for. The password should not be shared with any other team member at any time.

Best practice guidance dictates that regular audits should be completed to ensure that the CCTV system is only used in line with this policy. It is the responsibility of the Data Protection Officer (or their nominee) to complete the organisation's CCTV audit annually. If there have been any changes to the CCTV system i.e., change of location, further cameras added, consideration should be given to whether the CCTV should be re-audited, if changes are significant.

All team members should know how to respond to any queries about CCTV, if asked which includes:

- Where the CCTV cameras are located.
- The length of time images are held for.
- The purposes of the CCTV i.e., for crime prevention and safety.
- Who to contact to make a subject access request.

6.4 Storing and viewing CCTV images

Recorded material should be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. Recording units should be kept in a secure, lockable office/room. Images should be encrypted to prevent unauthorised access to images processed in a surveillance system.

Viewing live images should be restricted to authorised team members where it is necessary for them to see it, for the purpose of crime prevention and safety. Recorded images should also be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised team members.

6.5 Disclosure

Disclosure of information from surveillance systems must be controlled and consistent with the purpose of crime prevention and safety, for which the system was established. It is always acceptable to disclose information to law enforcement agencies as, failure to do so, would be likely to prejudice the prevention and detection of crime. The Data Protection Officer should be notified when CCTV images have been requested by a law enforcement authority.

Any other requests for information should be approached with care as wider disclosure may be unfair to the data subjects concerned. In some limited circumstances it may be appropriate to release information to a third party, where their needs outweigh those of the individuals whose information is recorded. In these circumstances, the Data Projection Officer should be consulted prior to images being released to said third parties.

6.6 Subject access requests

CCTV images should be disclosed if requested via a subject access request. CCTV images should be dealt with in the same way as paper or other electronic data. However, if the data subject agrees, a viewing of the footage is permitted instead of sending the images electronically. It will be necessary to obscure the images of other data subjects contained in the footage. Not doing so, would be considered a personal data breach that may be reportable to the Information Commissioner's Office.

Within Hallmark Care Homes, the team should report requests to the General Manager and log the request using the 'subject access request' workflow in RADAR. Subject access requests relating to Santhem Residences and Santhem Care should be reported to the General Manager and Data Protection Officer, by email, on dpo@hallmarkcarehomes.co.uk.

All requests should then be dealt with in line with the Hallmark Individual Rights and Data Access policy and procedure.

6.7 Retention

All CCTV systems should be inbuilt with an automatic retention period of no more than 30 days. Many of Hallmark Care Homes' systems have this feature in built and images are automatically overwritten on their 31st day. This feature should not be amended without the approval of the Executive Leadership Team and Data Protection Officer.

6.8 Keeping people informed

Signage for internal cameras

People must be informed when they are in an area where a CCTV surveillance system is in operation. The most effective way of doing this is by using signs displayed in prominent places. Signs should be displayed in areas before people enter the surveillance areas. The signs should then be repeated in the area that is being monitored by CCTV. Signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signage for external cameras

Signs must be displayed in order to alert drivers to the use of cameras in areas that vehicles have access to, such as car parks. It is important that these signs do not affect the safety of road users. Signs must make clear that cameras are in use and explain who is operating them,

so that individuals know who holds information about them and therefore have the opportunity to make further enquiries about how their data is being processed. Signage must also be displayed prior to data subjects entering the surveillance area.

There must be regular signage displayed to highlight individual's attention to other external cameras covering building areas.

6.9 Surveillance technologies other than CCTV

Surveillance technologies can also include automatic number plate recognition (ANPR), body worn video (BWV), unmanned aerial systems (UAS); and other systems that capture information of identifiable individuals or information relating to individuals. The Hallmark Care Homes Group of companies does not permit the use of any of these surveillance technologies, other than closed circuit television (CCTV).

6.8.1 Acoustic monitoring

A number of care home services have introduced acoustic monitoring. Acoustic monitoring is an innovative solution which uses sound detecting devices which alert team members, if residents require assistance. The system monitors audio only. No video or images will be captured of any resident who uses this system. Over time, the system will build a profile of participating residents, so that it can alert the team to any behaviours i.e., breathing or movements, that are variations from normal. Acoustic monitoring may not be suitable for all residents. Whether it is or not, will depend on the resident's individual circumstances and the risk(s) associated with their particular medication condition(s).

Appropriate consent must be sought and/or the requirements of the Mental Capacity Act 2005 must be followed in full, prior to the introduction of acoustic monitoring. Specific guidance relating to the use of acoustic monitoring has been developed and is included in appendix 2 of this policy. The relevant consent/agreement forms are also included in appendices 3 and 4.

6.10 Equipment installed/provided by residents or relatives

6.10.1 Surveillance equipment

We understand that people may sometimes worry about a resident and the care they receive. Any concerns can be raised with the team, and these will be dealt with in line with the requirements of our Feedback policy and procedure. A copy of our Feedback procedure can be found on our website here.

However, the introduction of covert or overt surveillance, by residents or their families, brings with it a number of data protection concerns. Most of all, the use of such equipment, particularly in residents' bedrooms, can impact on a resident's right to privacy and dignity.

Should surveillance equipment be discovered in a resident's bedroom, the team will notify the General or Duty Manager and Data Protection Officer as a matter of urgency. The resident's interests must be the key focus and any decision to turn off or remove equipment should be

made, with this in mind. Consideration should also be given to whether the use of the equipment is intruding on the privacy or rights of others and whether there is anyone who should give their consent to it being used.

The General or Duty Manager should discuss the equipment with the resident or their family, to determine whether they have any cause for concern. Any concerns should be investigated in line with our Investigation and Feedback policies.

General Manager's can decide to turn off surveillance equipment or remove it from a resident's room, keeping it safe until it can be returned to its owner. However, under no circumstances should this equipment be deliberately damaged or removed with the intention of not returning it. Neither should recordings be deleted.

6.10.2 Smart devices

Smart devices provide many benefits to residents and their families. It enables them to maintain contact, which enhances residents' wellbeing. We will always support residents (or their families) who wish to introduce and use smart devices within their bedrooms. However, residents (or their families) should discuss the intended use of such a device with the General Manager, prior to its introduction.

Any smart device which records or transmits live video images/voice recordings or which automatically answers video calls will, largely, be disabled by the team whilst they are supporting residents with personal care. This ensures that the dignity and privacy of the resident is upheld and maintained. Team members will also need to be informed of the intended use of these type of devices, and appropriate signage should be displayed on the resident's bedroom door to inform people that this type of device is in use.

Any concerns or queries from residents, their families or team members regarding the use of smart devices, should be shared with the Data Protection Officer, who will respond accordingly.

7. TRAINING AND OTHER RESOURCE IMPLICATIONS

Team members who regular handle personal data, including relevant Central Support team members and General Managers, will all receive face to face training in the application of policies and procedures linked to UK GDPR. This training will be refreshed at on an annual basis. Additional face to face training (for new team members who require this level of training) will be provided by the DPO.

Other team members who do not receive the initial face to face training, will receive GDPR training via an e-learning platform. The policy awareness questionnaire/quiz (see appendix 1) can be used to ensure that team members have read and understood the content of this policy.

GDPR training (regardless of delivery) will be mandatory and will refreshed on an annual basis. All new team members will read the policies on data protection and on confidentiality as part

of their induction process.

Senior team members will monitor the application of this policy via audit and observation.

Failure to adhere to the process as defined in this policy will be addressed via supervision or performance management processes.

Appendix 1

Policy awareness quiz: CCTV and surveillance policy (v3)

Team member name:	
Work location:	
Date:	

Please put a tick next to the correct answer to each question.

1. What does CCTV stand for?	
a. Closed-circuit television	
b. Automatic number plate recognition	
c. Body worn video	
d. Unmanned aerial system	
2. What is the reason or purposes for which we use CCTV at Hallmark?	
a. Monitoring of residents.	
b. Monitoring of team members.	
c. Crime prevention and safety.	
d. For oversight of our facilities.	
3. Who should any requests for access to CCTV images, be directed to? *(Choose 2)*	
a. General Manager	
b. Line Manager	
c. Data Protection Officer	
d. Regional Director	
4. How long should CCTV images be retained for?	
a. No more than 7 days	
b. No more than 14 days	
c. No more than 28 days	
d. No more than 30 days	
5. What are the main ways in which people can be kept informed of the user of CCTV?	
a. Signage	
b. Verbally	
c. Letter	
d. Email	
6. What areas, are permitted to be covered by CCTV? *(Choose 2)*	
a. Corridors	
b. Key entrances	
c. Grounds and car park	
d. Resident's bedrooms	

Appendix 1

7. The requirements of what legislation should be followed, prior to the introduction of acoustic monitoring?	
a. UK GDPR	
b. Data Protection Act	
c. Mental Capacity Act	
d. None	
8. Should surveillance equipment be identified in a resident's room, who should be notified? *(Choose 2)*	
a. General/Duty Manager	
b. CQC/CIW	
c. The ICO	
d. Data Protection Officer	

Once completed, please hand to your line manager.

For completion by line managers/assessors only:

Score out of 11 (pass mark is 8+):	
Passed:	**Yes / No**
Marked by (name):	
Date:	

For completion by the Business Administrator:

Uploaded to Your Hippo (date):	

Appendix 2

Data protection guidance for team members: acoustic monitoring (v3 of the CCTV and surveillance policy)

This guidance has been developed to ensure that we have the correct authority to introduce acoustic monitoring into the rooms of residents.

Acoustic monitoring is an innovative solution which will alert team members, if residents require assistance. The system monitors audio only. No video or images will be captured of any resident who uses this system. Over time, the system will build a profile of participating residents, so that it can alert the team to any behaviours i.e. breathing or movements, that are variations from normal.

That said, acoustic monitoring may not be suitable for all residents. Whether it is or not, will depend on the resident's individual circumstances and the risk(s) associated with their particular medication condition(s).

The guidance varies, depending on whether:

1. The resident has capacity.
2. The resident lacks capacity but has a registered Lasting Power of Attorney for Health and Welfare.
3. The resident lacks capacity and does not have a registered Lasting Power of Attorney in place.

Please click on the links above, to be taken to the relevant part of the guidance.

Appendix 2

1. The resident has capacity.

If a resident has capacity and wants to have acoustic monitoring in their room, they should complete the 'Consent form: acoustic monitoring'. The resident should read the one page 'Consent information', prior to completing the consent form. Resident's do not need to consent to the use of acoustic monitoring, if they do not want it in their room.

If the resident wants the acoustic monitoring system in their room, they should complete the 'Consent form':

- The resident should tick the box labelled 'I consent to the use of acoustic monitoring in my bedroom'.
- The resident should then tick one on the final three boxes to choose whether:
    - They consent to the system being 'active' 24 hours a day.
    - They consent to the system being 'active' at night-time only (between 20:00 and 08:00).
    - They consent to the system being 'active' at other times. If this box is ticked, the resident should state in the next box, the times they do want the system activated.
- The resident should then write their name in the relevant box.
- The resident should then sign and date the form.
- They should also tick to confirm that they have read, understood and agree to the 'Consent Information'.
- The resident should also tick to confirm that they have been shown how to activate and deactivate the system. A team member should show them how to do this, prior to the consent form being given to the resident to sign.

Once completed, a copy of the form should be scanned and added to the documents section of iCare or Kare Inn.

Appendix 2

2. The resident lacks capacity but has a registered Lasting Power of Attorney for Health and Welfare.

If a resident has been assessed as lacking the capacity to consent to the decision to introduce acoustic monitoring in their room, but they have a Lasting Power of Attorney for Health and Welfare, the attorney can agree to this if they deem it to be in the resident's best interests.

If the attorney does deem it to be in the resident's best interests, they should complete the 'Agreement form: acoustic monitoring'. The attorney should read the one page 'Agreement information', prior to completing the form. Attorney's do not need to agree to the use of acoustic monitoring, if they do not feel it would be in the resident's best interests.

If the Attorney deems acoustic monitoring to be in the resident's best interests, they should complete the 'Agreement form':

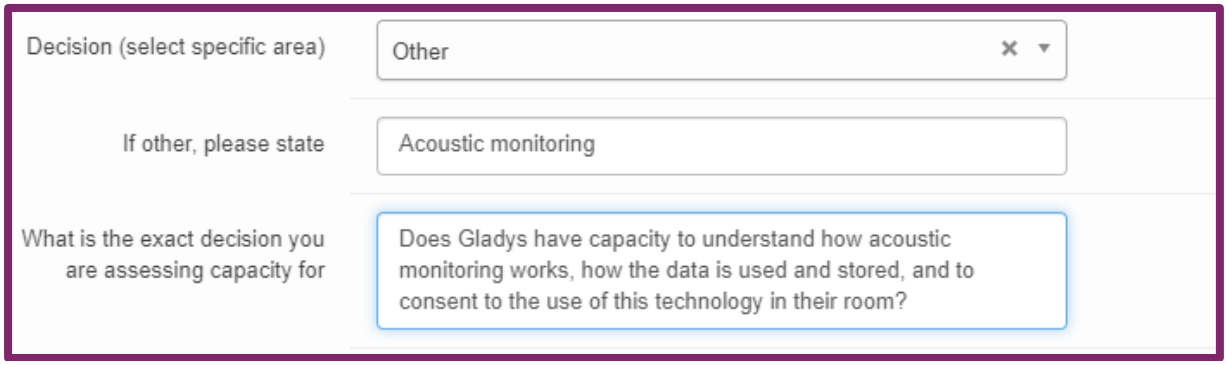
- The attorney should tick the box labelled 'I agree to the use of acoustic monitoring in the residents' bedroom. I believe that use of the system is in their best interests'.
- The attorney should then tick one on the final three boxes to choose whether:
    - They agree to the system being 'active' 24 hours a day.
    - They agree to the system being 'active' at night-time only (between 20:00 and 08:00).
    - They agree to the system being 'active' at other times. If this box is ticked, the attorney should state in the next box, the times they do want the system activated.
- The attorney should then write their name in the relevant box.
- The attorney should write the resident's name in the appropriate box.
- The attorney should then sign and date the form.
- They should also tick to confirm that they have read, understood and agree to the 'Agreement Information'.

Once completed, a copy of the form should be scanned and added to the documents section of iCare or Kare Inn.

Appendix 2

3. The resident lacks capacity and does not have a registered Lasting Power of Attorney in place.

If a resident has been assessed as lacking the capacity to consent to the decision to introduce acoustic monitoring in their room and they do not have a Lasting Power of Attorney for Health and Welfare, an assessment should be undertaken to determine whether the introduction of the monitoring is in the resident's best interests (as per the MCA/DoLs policy). The assessment should be focused on that individual resident and the risk(s) associated with their medical condition(s). This assessment should be recorded on the 'Care Assessment - Best Interest Decision- Mental Capacity Act (MCA)' form in iCare, as below:



For homes using Kare Inn, a mental capacity assessment should be recorded in the system. The specific issue/context requiring an assessment of capacity should be recorded as 'Does <resident name> have capacity to understand how acoustic monitoring works, how the data is used and stored, and to consent to the use of this technology in their room?'.

The rest of either assessment (whether it be on iCare or Kare Inn) should be completed, as per the prompts on the form. The assessment should include:

- The views (both past and present) of the resident, as much as possible.
- The views of any family members or friends involved in the resident's care, where applicable.
- The views of any health and social care professionals, where relevant.

When determining the outcome of the decision, the following factors must be borne in mind:

- If acoustic monitoring is being considered because the resident is at high risk of falls, where have they previously fallen? Has this been in their bedroom or communal areas? If the resident has fallen in communal areas, acoustic monitoring would not mitigate the risk of this reoccurring.
- If acoustic monitoring has been deemed to be in the resident's best interests, have the times the monitoring is going to be active, been considered? I.e. if the resident has a history of falling in the day and not at night, does the resident need acoustic monitoring activated at night?

It is important to determine whether the introduction of acoustic monitoring, will mitigate the identified risk(s).

Appendix 3

Consent form: acoustic monitoring

Data Controller name:	
Retention period	3 months from the date of recording.

For completion by the data subject/resident

Processing activity	For completion by the data subject/resident **If you consent to the use of acoustic monitoring, please tick the box below.**
I consent to the use of acoustic monitoring in my bedroom.	☐
If you have ticked the box above, please tick one of the boxes below as well, to indicate the times that the monitoring is active.	
I consent to the acoustic monitoring system being 'active' 24 hours per day.	☐
I only consent to the acoustic monitoring system being 'active' at night (from 20:00 to 08:00)	☐
I only consent to the acoustic monitoring system being active during other times. *Please specify these in the box below.*	☐
If you would only like the acoustic monitoring system active at certain times, please state these below:	

Name:	
Date:	
Signature:	
I have read, understood and agree to the 'Consent Information' (version 2) overleaf. *Please tick the box to the right to confirm.*	☐
I have been shown how to activate and deactivate the system. *Please tick the box to the right to confirm.*	☐

Once complete, this form should be scanned and uploaded to the documents section of iCare/Kare Inn.

Appendix 3

Consent Information

This information should be read prior to signing the consent form.

The Hallmark Care Homes group of companies are introducing acoustic monitoring in its care homes. This means that a small monitoring device is installed in your bedroom, which will alert the team if you need assistance. You are able to activate and deactivate the system yourself and a Hallmark team member will have shown you how to do this. The system monitors audio only. No video or images will be captured of any resident who choose to use this system. Over time, the system will build a profile of you, so that it can alert the team to any behaviours i.e. breathing or movements, that are variations from normal.

Please note that the team cannot monitor your room on a continuous basis. The team can only listen to recordings when the system alerts them to variations from normal.

Please note that you do not have to consent to the use of acoustic monitoring. If you do not wish to give us consent, this will not be recorded anywhere and will not impact our relationship with you.

If you do wish to consent, the data will be stored for the length of time stated on the consent form. This is referred to as the 'retention period'.

1. The identity of the data controller

The identity of the data controller is stated on the consent form. A data controller is 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 UK GDPR.

2. The processing activities

The processing activity is the use of acoustic monitoring, as stated on the consent form. If you consent to the use of acoustic monitoring, you are also able to consent to specify the duration that this monitoring system is active. However, please note that the monitoring system is predominantly only used during the night.

3. The right to withdraw consent

Just because you have consented now, does not mean that you can't change your mind in the future. If you would like to withdraw your consent, you can do so at any time. To withdraw your consent, please contact the General Manager.

Appendix 4

Agreement: acoustic monitoring

Data Controller name:	
Retention period	3 months from the date of recording.

For completion by an attorney holding Lasting Power of Attorney for Health & Welfare for the resident

Processing activity	For completion by the resident's LPA for Health and Welfare **If you believe acoustic monitoring is in the donor/resident's best interests and agree to its use, please tick the box below.**
I agree to the use of acoustic monitoring in the residents' bedroom. I believe that use of the system is in their best interests.	☐
If you have ticked the box above, please tick one of the boxes below as well, to indicate the times that the monitoring is active.	
I agree to the acoustic monitoring system being 'active' 24 hours per day.	☐
I only agree to the acoustic monitoring system being 'active' at night (from 20:00 to 08:00)	☐
I only agree to the acoustic monitoring system being active during other times. *Please specify these in the box below.*	☐
If you would only like the acoustic monitoring system active at certain times, please state these below:	

Resident's name:	
Name of LPA:	
Date:	
Signature:	
I have read, understood and agree to the 'Agreement Information' (version 2) overleaf. *Please tick the box to the right to confirm.*	☐

Once complete, this form should be scanned and uploaded to the documents section of iCare/Kare Inn.

Appendix 4

Agreement Information

This information should be read prior to signing the agreement form.

The Hallmark Care Homes group of companies uses acoustic monitoring in its care homes. This means that a small monitoring device is installed in your bedroom, which will alert the team if residents need assistance. The system can be activated and deactivated and a Hallmark team member can show you how to do this. The system monitors audio only. No video or images will be captured of any resident who choose to use this system. Over time, the system will build a profile of each resident, so that it can alert the team to any behaviours i.e. breathing or movements, that are variations from normal.

Please note that the team cannot monitor rooms on a continuous basis. The team can only listen to recordings when the system alerts them to variations from normal.

Please note that you do not have to agree to the use of acoustic monitoring. If you do not wish to agree, this will not be recorded anywhere and will not impact our relationship with you or the resident.

If you do wish to agree, the data will be stored for the length of time stated on the agreement form. This is referred to as the 'retention period'.

4. The identity of the data controller

The identity of the data controller is stated in the agreement. A data controller is 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 UK GDPR.

5. The processing activities

The processing activity is the use of acoustic monitoring, as stated in the agreement. If you agree to the use of acoustic monitoring, you are also able to agree to specify the duration that this monitoring system is active. However, please note that the monitoring system is predominantly only used during the night.

6. The right to withdraw permission

Just because you have agreed now, does not mean that you can't change your mind in the future. If you would like to withdraw your permission, you can do so at any time. To withdraw your permission, please contact the General Manager.