HEALTHSHARE PRIVACY NOTICE

Policy Domain	PN
Policy ID	PN 001
Version Number	7
Authors	Les De-Lara
Job Title	Information Governance Lead
First Release Date	10/10/2012
Ratification Date	20/08/2021
Ratified By	IT Steering Group
Implemented By	IT Steering Group
Audit and Review By	IT Steering Group
Review Frequency	Triennially
Last Review Date	05/08/2021
Next Review Date	By 01/08/2024

Table of Contents

PRIVACY NOTICE FOR HEALTHSHARE

1 LAWFUL REASON TO USE YOUR PERSONAL INFORMATION

Healthshare (or the GP referring you) is required to have a lawful reason to use your personal data. There are 6 lawful reasons and we generally use the provision of direct care under GDPR Article 6(1)(e) – the performance of a task carried out in the public interest for processing and for special category data GDPR Article 9(2)(h) – medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

There will also be some occasions that we will require your explicit consent GDPR Article 6(1)(a) – explicit consent and for special category data GDPR Article 9(1)(a) – explicit consent. We will record your consent to use your personal information in your patient record in our Patient Administration System. The consent may be under the confidentiality of data and may not be the same as the lawful basis we are processing that data.

At any time, you can inform us that you no longer wish us to use your personal information. Whilst it is not a precondition of receiving your service, the Healthshare clinicians and other staff have a duty to care for you safely. If they cannot ensure your care safety with the withdrawal of your information which they need, they may well discharge you from the Service and ask you to return to your GP.

This course of action is of course a last resort and Healthshare will endeavour in all circumstances to continue your care.

2 NATIONAL DATA OPT OUT

We are committed to keeping patient information safe and always being clear about how it is used.

All health and care organisations are required to be compliant with the National Data Opt-Out policy. This means you can choose to stop your confidential patient information being used for research and planning. You can also make a choice for someone in your care, such as your children under the age of 13.

Your choice will only apply to the health and care systems in England.

You can view and change your national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters or by calling 0300 3035678.

To ensure that we are compliant with the national opt-out guidelines, we reviewed our processes and implemented systems to allow us to remove records of service users who wish to opt-out of sharing their confidential patient information for research and planning.

You can find out more information about national data opt-out on This Patient Leaflet

3 HOW WE USE YOUR PERSONAL INFORMATION

This fair processing notice explains why Healthshare collects information about you and how that information may be used.

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g., NHS Trust, GP Surgery, Healthshare clinics, etc.). These records help to provide you with the best possible healthcare.

Health records may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Those records that

are Special Category under the law and as such our responsiveness to handle and process your personal data are even more sensitive. Records which Healthshare hold about you may include the following information:

- Details about you, such as your address and emergency contact details
- Any contact the service has had with you, such as appointments and clinic visits
- Notes and reports about your health
- Recordings of your telephone calls
- Details about your treatment and care
- Results of investigations such as laboratory tests and x-rays
- Relevant information from other health professionals, relatives or those who care for you

To ensure you receive the best possible care, your records are used to inform the care you receive. Information held about you may be used to help protect the health of the public. Information may be used within the service for clinical audit to monitor the quality of the service provided and protection of Healthshare staff.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified.

4 HOW DO WE MAINTAIN THE CONFIDENTIALITY OF YOUR RECORDS?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- General Data Protection Regulation (GDPR) 2018
- Data Protection Act 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality and Information Security
- Information Governance: To Share or Not to Share Review.

5 ACCESSING YOUR RECORDS

Every member of staff who works for Healthshare has a legal obligation to keep information about you confidential. Individual staff may only view your records with a legitimate reason for a legitimate purpose. This would of course include the clinician(s) directly involved in your care or other staff who might be ordering or receiving results linked to your care.

Other administration or management staff may need to access and use your records to contact you regarding appointments or your care. Our Patient Administration System where your records are stored creates a record of who has accessed your record for control and audit purposes.

Accessing or allowing someone else to access, your record without a legitimate purpose by a Healthshare member of staff is a serious data breach and is dealt with under our disciplinary procedures and reported to the Information Commissioners Office.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any 3rd party without your explicit consent unless there are exceptional circumstances (i.e., life or death situations), where the law requires information to be passed on and / or in accordance with the new information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where 'The duty to share information can be

as important as the duty to protect patient confidentiality.' This means that healthcare professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles. This is supported by our policies, regulators and professional bodies.

6 RESEARCH AND PLANNING

Healthshare takes part in research that uses anonymised or pseudonymised data. It also takes part in planning at a local, regional and national level. Data which is anonymised or pseudonymised data means that it cannot be traced back to an identifiable individual and is therefore no longer personal data under the 2018 Data Protection Act and thus preserves patient privacy and confidentiality.
Anonymised or pseudonymised patient data held by Healthshare may also be used to evaluate present services that provide direct care or to plan future ones within the practice or across the local area. Sometimes, Healthshare is contacted to ask whether its patients would consider taking part in research on a particular condition, but where the data used would identify those individuals. In all such cases, identifiable patient data will only be used where patients have given their consent.

7 SUBJECT ACCESS REQUEST

You have a right under the General Data Protection Regulation (GDPR) 2018 to request access to obtain copies of what information the service holds about you and to have it amended should it be inaccurate. A Subject Access Request (SAR) is an important facet of GDPR and is likely a future privacy law. It is what allows you to request and receive a copy of your personal data. Healthshare must comply with an SAR without undue delay and at the latest within one month of receiving your request. Your data is provided without cost to you.

In order to request this, you need to do the following:

Your request can be made by completing our online form. We will request to see proof of your identity because the teams dealing with your request are not at the clinic you visit and they must be absolutely sure you are who you say you are. If you have further questions, please email ig@healthshare.org.uk

This method of obtaining your request is secure.

8 VERIFYING YOUR IDENTITY

We are required to verify your identity each time you contact us. You will be asked to provide identity information (for example full name, address, date of birth and NHS number) so your records can be located. We may also request a photo ID.

If you wish a spouse, relative or carer to communicate with us on your behalf we will need to obtain your explicit consent before doing so.

Where we use your personal data

Your personal data is stored securely within the United Kingdom in databases accessed with multiple levels of security. This ensures that only authorised Healthshare staff access your record.

The databases are held on IT systems using highly secured equipment, software and security which are located in Data Centres and backed up off-line.

Data is transmitted using the NHS mandated network that is appropriately encrypted to NHS Standards.
Data in our Patient Administration Systems are not stored outside of the United Kingdom.

9 YOUR RIGHT TO HAVE YOUR RECORDS CHANGED

You have a right to have inaccurate personal data rectified or completed if it is incomplete. Clinical notes and clinical opinions will not generally be altered but may of course be supplemented by additional personal data.

10 WHO ARE OUR PARTNER ORGANISATIONS?

We may also have to share your information, subject to strict agreements and your consent on how it will be used, with the following organisations:

- NHS Trusts / Foundation Trusts
- General Practitioners/Consultants
- NHS Commissioning Support Units
- Clinical Commissioning Groups
- Private Sector Providers
- Other 'data processors' which you will be informed of

If your data is shared outside of direct care, you will be asked for explicit consent for this if this is required. In all circumstances we will transit your personal data securely. In almost all instances the transfer of your data will be electronic either through the encrypted NHS network, or using NHS.net secure encrypted email or through an NHS encrypted portal (e.g., enabling an x-ray result to be shared between Healthshare and NHS organisations).

11 HOW WE WILL COMMUNICATE WITH YOU

In order to communicate with you, we are likely to do this by telephone, SMS, email, and/or post. If we contact you using the telephone number(s) which you have provided (landline and/or mobile), and you are not available which results in the call being directed to a voicemail and/or answering service, we may leave a voice message on your voicemail and/or answering service as appropriate.

Any message left will be discrete and will not contain confidential information. In almost all circumstances the message will simply ask you to contact us.

In your initial patient registration with us we will seek your consent to contact you and via which route. If your preference for how we communicate with us changes please contact us so that we may amend your preferences.

12 RIGHT OF ACCESS TO PERSONAL INFORMATION

You have a right under the General Data Protection Regulation (GDPR) to request access to obtain copies of what information the service holds about you and to have it amended should it be inaccurate. Your data is provided without cost to you. In order to request this, you need to do the following:

Your request can be made to the Service in person in the clinic, on the telephone or using this link https://forms.office.com/r/HKX6dzsuuH We are required to respond to you within 30 days.

13 RETAINING YOUR PERSONAL INFORMATION

Unlike many other types of personal information, under GDPR there is no 'Right to Erasure' of Health records. Indeed, the Health Act requires us to retain your records for a minimum of 8 years after we have finished your care (discharge). Where your care record is part of your GP record retention is for a minimum of 20 years or 8

years post death. We are of course still bound by the strict rules of GDPR on how we store, access and release your patient information.

14 MARKETING AND OTHER PROMOTIONAL CONTACT

Healthshare is commissioned to provide your service. We will never contact you to promote either other Healthshare services or those of a third party. If you are contacted by someone purporting to represent Healthshare please report it immediately to our Data Protection Officer DPOfficer@Healthshare.org.uk who will deal with the matter.

15 OBJECTIONS AND COMPLAINTS

Should you have any concerns about how your information is managed, please contact the Service Manager or our Data Protection Officer. If you are still unhappy following interaction with Healthshare, you can then complain to the Information Commissioners Office (ICO) via their website (www.ico.gov.uk).

16 DATA PROTECTION OFFICER

You are able to contact our Data Protection Officer by e-mail.

If you do not get a satisfactory response from the Data protection Officer then you should contact the supervisory authority. In UK this is the Information Commissioners Office (ICO), they can be contacted on 03031231113

17 CHANGE OF DETAILS

It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

The General Data Protection Regulation 2016 requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information. Healthshare is registered with the Information Commissioners Office (ICO).

This information is publicly available on the Information Commissioners Office website www.ico.org.uk.

18 WHAT YOU NEED TO DO NOW

If you are happy for your data to be extracted and used for the purposes described in this fair processing notice then you do not need to do anything.
If you do not want your personal data being extracted and leaving the service for any of the purposes described, you need to let us know as soon as possible.

19 PRIVACY NOTICE CCTV (CLOSED CIRCUIT TELEVISION) DATA

This Privacy Notice explains the kind of personal data Healthshare collects from you when visiting any of our sites with CCTV in operation and how Healthshare uses this data.

19.1 Why we collect personal data?

Healthshare collects data through the CCTV system for various reasons:

- To control access to the building and to ensure the security of the building, the safety of Healthshare staff and visitors, as well as property and information located or stored on the premises
- To prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information
- To prevent, detect and investigate theft of equipment or assets owned by Healthshare, visitors or staff or threats to the safety of personnel working at the office (e.g., fire, physical assault).

The CCTV system is not used for any other purpose, such as to monitor the work of employees or their attendance. It is important to notice that the location and positioning of the video-cameras are such that they are not intended to cover the surrounding public space; the cameras are aimed to give a general overview of what`s happening in certain places but not to recognise persons.

The system is also not used as an investigative tool or to obtain evidence in internal investigations or disciplinary procedures unless a security incident is involved. (In exceptional circumstances, the data may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation). The CCTV cameras are installed at the entrances, placed and focused in a way that only people who want to access the site or the annexed facilities including parking areas property are filmed.

The CCTV system covers the area of entry and exit points of the building, entry points inside the building, delivery, and outer area of the building.

19.2 What kind of data does Healthshare collect?

Healthshare collects just images caught on camera, and no voice is recorded.

19.3 Who is responsible for the processing of the data?

Healthshare is the legal entity who initiated the processing of personal data and who determines the objective of this processing activity. Moreover, the Information Governance Lead is responsible for this operation.

19.4 Which is the legal basis for this processing operation?

Healthshare uses video-surveillance equipment for security and access control purposes, which is an action necessary for the management and functioning of Healthshare. Therefore, the processing is lawful under Article 5(a) of the Regulation (EC) No 45/2001.
Carrying out video-surveillance is necessary for compliance with a legal obligation of EU law to which Healthshare is subject. Therefore, the processing is lawful under Article 5(b) of the Regulation (EC) No 45/2001.
In addition, at the entrance there is one on-the-spot-notice about the video-surveillance activity, clearly visible so in this case using the specific sign-posted part of the facility may constitute the fact that the processing is lawful under Article 5(d) of the Regulation (EC) No 45/2001 because “the data subject has unambiguously given his or her consent”.

19.5 Who can see my data?

The images can be accessed by the operation, IT and Information Governance staff members of Healthshare and by the contracted security company. Access to the hard-disc recorder is highly limited, being protected by a password and recording any log or action from the staff members. The data cannot be accessed without the authorisation of the Information Governance Lead.

19.6 How to control your data?

You can send an email request to IG@healthshare.org.uk

19.7 Can I access my data?

You have the right to access your data at any time and free of charge, by sending an email request to IG@healthshare.org.uk.

19.8 Can I modify my data?

Modifying the CCTV footage is not allowed. However, you can modify the report written by the operation staff in connection with a security incident, if applicable in your case.

19.9 Can I block you from processing my data?

You have the right to block the processing of your personal data at any time by sending an email request to IG@healthshare.org.uk when you contest the accuracy of your personal data or when Healthshare no longer needs the data for completing its tasks. You can also block the processing activity when the operation is unlawful, and you oppose to the erasure of the data. However, blocking is not possible in case of an official investigation.

19.10 Can I delete my data?

You have the right to delete your data at any time by sending an email request to IG@healthshare.org.uk when the processing activity is unlawful.

19.11 Do you share my data with other organisations?

We keep your data inside Healthshare unless you ask us or give us your permission to share it. In case we share your data with third parties, you will be notified to whom your personal data has been disclosed.

19.12 Do I have the right to object?

Yes, you have the right to object at any time by sending an email request to IG@healthshare.org.uk when you have legitimate reasons relating to your particular situation. Moreover, you will be informed before your information is disclosed for the first time to third parties, or before it is used on their behalf, for direct marketing purposes.
Healthshare will confirm your requests within 21 days from the receipt of the request.

19.13 What can I do in the event of a problem?

The first step is to notify Healthshare by sending an email to IG@healthshare.org.uk and ask us to take action.
The second step, if you obtain no reply from us or if you are not satisfied with it, contact our data protection officer (DPO) at dpofficer@healthshare.org.uk.
At any time, you can lodge a complaint with the Information Commissioners Office on 0303 123 1113, who will examine your request and adopt the necessary measures.

19.14 When will we start the processing operation?

We will start the processing operation when you are visiting Healthshare`s premises with CCTV.

19.15 Security of personal data

Healthshare is committed to protecting the security of your personal data. Therefore, we use several security technologies and procedures to help us to protect your personal data from unauthorised access, use or disclosure. We keep your data on computer systems that are limited access and just in controlled facilities.

19.16 How long do we keep your data?

Healthshare will keep your personal data for 28 calendar days after your visit to our premises. After that period any CCTV recorded footage is automatically deleted.