Bevan Healthcare

Health - Hope - Humanity

BEVAN HEALTHCARE

Privacy Notice

May 2018

Approval Date: May 2018

Review Date: May 2019

This policy should be reviewed every 1 year, or earlier if changes in policy occur.

Confidentiality Notice

This document and the information contained therein is the property of Bevan Healthcare CIC.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Bevan Healthcare CIC.

Document Details

Classification:	Operational
Author and Role:	Beth Kirby
Organisation:	Bevan Healthcare CIC
Document Reference:	Privacy Notice
Current Version Number:	V1.1
Current Document Approved By:	
Date Approved:	

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
V.1	23.05.2018	**Beth Kirby - Approved by Bradford CCG's eDSM group**	Karen Naylor	

Contents

Introduction to Policy

This document is to explain to you the types of personal data we hold about you and how we may use this information for the benefit of your health and wellbeing. The document advises you on how we allow [or do not allow] your electronic health record to be made available to other organisations, across a variety of healthcare settings. This is subject to your permission, being made on the computer system SystmOne. It informs you of your options should you wish to take further control of your SystmOne record. The information should be carefully considered and any concerns you have about the data we hold, and how we use it, should be raised with us.

1. The information we hold about you

As your registered GP practice we hold your electronic health record. This contains sensitive information about you, your health and your wellbeing. The following list provides an example of the type of information (both past and present) that can be held within your record:

- Demographic and contact details (name, date of birth, address, telephone number, email address, gender, sex, religion, marital status etc.)
- Appointments and consultations
- Diagnoses (including physical disabilities and mental health conditions)
- Medication, vaccinations, pathology results (e.g. blood tests) and allergies
- Hospital correspondence and correspondence from other health and social care settings (including x-rays, discharge letters and referrals)
- Relationships/next of kin

2. Why do we [and other organisations] need access to your personal data?

This information means we can provide you with high quality direct care in a safe and effective manner. Being able to see your detailed record allows for an overall picture of your health and wellbeing to be assessed. This then helps us to diagnose and prescribe appropriate courses of

treatment to you. This means that the most safe and efficient care is provided to you. We do not want you to have to repeat your medical history and remember every detail, which may or may not be relevant, to every health professional involved in your care. Lack of access to your information may lead to misdiagnosis, inappropriate prescribing of medication or tests and/or ineffective treatment.

We recognise that you will benefit from other health providers that care for you (either currently or in the future) having access to your electronic health record. This is because they can then make fully informed decisions about the care you require. The reasons for access to the detailed record, mentioned above, apply across the health profession. A shared record ensures that care providers always have the most accurate, up to date information.

In a case where patient data is required for research purposes, we do not provide patient identifiable information. Any data we provide is anonymised or pseudonymised, unless you have given explicit consent.

Anonymised data, is data about you but from which you cannot be personally identified. Anonymised data is any personal data which has been processed so that all identifiers (such as name or NHS number) are removed, minimising the likelihood that the data will identify individuals.

Pseudonymised data is any personal data which has been processed so that all identifiers such as name, address, date of birth and NHS number is removed and replaced with a code which makes it anonymous to those who should not see your identifiable data, but would allow others such as those responsible for providing care to identify an individual.

Personal identifiable data, is data which relates to a living individual who:

- can be identified either from that data; or
- from that data in conjunction with other information within the possession of the data controller

Purpose of using personal data	Legal basis of processing	Special category of data
Provision of direct care and related administrative purposes e.g., e-referrals to hospitals or other care providers	GDPR Article 6(1)(e) – the performance of a task carried out in the public interest	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.
For commissioning and healthcare planning purposes e.g., collection of mental health data set via NHS Digital or local	GDPR Article 6(1)(c) – compliance with a legal obligation	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. Special category 9(2)(i) – public interest in the area of public health

For planning and running the NHS (other mandatory flow) e.g., CQC powers to require information and records	GDPR Article 6(1)(c) – compliance with a legal obligation (the GP practice) Regulation 6(1)(e) – the performance of a task carried out in the public interest (CQC)	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. Special category 9(2)(i) – public interest in the area of public health
For planning & running the NHS – national clinical audits	GDPR Article 6(1)(e) – the performance of a task carried out in the public interest	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. Special category 9(2)(i) – public interest in the area of public health
For research	GDPR Article 6(1)(f) – legitimate interests…except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject. GDPR Article 6(1)(e) – the performance of a task carried out in the public interest GDPR Article 6(1)(a) – explicit consent	GDPR Article 9(2)(j) – scientific or historical research purposes or statistical purposes
For safeguarding or other legal duties	GDPR Article 6(1)(e) – the performance of a task carried out in the public interest Regulation 6(1)(c) – compliance with a legal obligation	GDPR Article 9(2)(b) – purposes of carrying out the obligations of ..social protection law.
When you request us to share your information e.g., subject access requests	GDPR Article 6(1)(a) – explicit consent	GDPR Article 9(1)(a) – explicit consent

3. What do we mean by 'Direct Care'?

The term 'Direct Care' means a clinical health activity concerned with the prevention and investigation and treatment of illness. It includes supporting your ability to function and improve your participation in life and society. It also includes the assurance of safe and high quality care and treatment undertaken by one or more registered and regulated health professionals and their team with whom you have a legitimate relationship for your care purposes.

It does not include access to information for purposes such as insurance, advertising or marketing.

4. How we share your personal data [our practice default]

As your GP practice we have set the following practice settings for all our registered patients whose detailed electronic health record is in our possession and within the clinical computer system, SystmOne. However, we recognise that each of our patients have differing health care needs and you may wish to control yourself how your personal data is shared. This can be done via '**Your Choice**' stated below.

A) Implied consent to make your record available to all organisations (without verification/ security process) for direct care purposes

We assume that you are happy to share your detailed electronic health record to those that care for you. We therefore, make your record available to all NHS commissioned services using the clinical record computer system, SystmOne. This allows for anyone at these organisations who have the appropriate controls to retrieve your electronic record once you are registered for care. However, these individuals should only legitimately access your record to provide you with care services. They must also record your permission to view your record.

AND/OR

B) Explicit consent to make your record available to all organisations (without verification/ security code process) for direct care purposes

We will obtain your explicit consent (permission) to share your detailed electronic health record to those that care for you. By providing your permission, we make your record available to all NHS commissioned services using the clinical record computer system, SystmOne. This allows for anyone at these organisations who have the appropriate controls to retrieve your electronic record, once you are registered for care. However, these individuals should only legitimately access your record to provide you with care services. They must also record your permission to view your record.

Your individual sharing preference will overwrite our organisation's default sharing setting.

<u>Bevan House Primary Care Centre</u>

The types of organisation who could be involved in your direct care and therefore need access to your electronic record are:

- All GP practices
- Referral triage and Out of Hours call centres (services determining which organisations should care for you)
- Child Health
- Urgent Care (for example A&E, Minor Injury Units and Out of Hours services)
- Palliative Care
- Prisons and custody suites or offender health
- Substance misuse service
- All NHS hospitals – acute and community

- Bradford Teaching Hospitals Foundation Trust
- Bradford District Care Trust services
- NHS Mental Health Services
- Community pharmacies

York Street Health Practice

- Leeds Hospital Foundation Trust
- Other national providers of healthcare who you choose to be referred to, in consultation with your healthcare professional
- Leeds & York Partnership Foundatoinal Trust
- Mid-Yorkshire Hospital Trust
- Leeds Community Healthcare Trust
- NHS National Diabetes Prevention Programme
- Local Care Direct
- Connect Well
- Reed Momenta
- Forward Leeds Partnership
- Calibre Health Partners Ltd
- Leeds City Council: Public Health, Adult or Child Social Care Services
- Embed Health Consortium (NHS commissioning support unit)
- Leeds Clinical Commissioning Group
- NHS Digital (Formerly known as (HSCIC)
- The "Clinical Practice Research Datalink" (EMISWeb practices) or ResearchOne Database (SystmOne practices).
- Other data processors which you will be informed of as appropriate.

Safeguarding and Exceptional Circumstances

For safeguarding purposes, life or death situations or other circumstances when we are required to share information:

We may also disclose your information to others in exceptional circumstances (ie life or death situations) or in accordance with Dame Fiona Caldicott's information sharing review (Information to share or not to share).

For example, your information may be shared in the following circumstances:

- When we have a duty to others e.g. in child protection cases

- Where we are required by law to share certain information such as the birth of a new baby, infectious diseases that may put you or others at risk or where a Court has decided we must.

Research

Research data is usually shared in a way that individual patients are non-identifiable. Occasionally where research requires identifiable information you may be asked for your explicit consent to participate in specific research projects. The surgery will always gain your consent before releasing any information for this purpose.

Where specific information is asked for, such as under the National Diabetes audit, you have the choice to opt of the audit.

The full list of organisations can be seen and updated in your patient online record.

To find out more about these types of organisations please go to the following webpage: http:// www.tpp-uk.com/products/systmone/modules or talk to a member of your GP practice.

If at any point in the future you are not happy to share your electronic record in this way, please let us know as soon as possible.

When you request to see your information or ask us to share it with someone else:
If you ask us to share your data, often with an insurance company, solicitor, employer or similar third party, we will only do so with your explicit consent. Usually the requesting organisation will ask you to confirm your consent, often in writing or electronically. We check that consent before releasing any data and you can choose to see the information before we send it.

5. Your choice

You may not agree with the health and social care organisations we have chosen to have access to your detailed electronic health record (the practice default). You can therefore control this yourself. **Your choice will override our settings.** You have the following options:

- **No organisations require you to provide a security code (Allowed List)** - You can give your permission to allow all NHS commissioned services and local authorities providing health services, using the clinical record computer system, SystmOne, to access your record. This allows for any individual at these organisations (who have the appropriate access controls) to retrieve your electronic record, only after you are registered with them for care. These individuals should only legitimately access your record to provide you with care services and they should always request and gain your consent before doing so.

- **All organisations require you to provide a security code (Verification List)** - You can require that all health organisations must ask you for a PIN number on your first visit to that service. This allows you to verify/confirm that each individual organisation should have access to your record, as they are legitimately involved in your care. You will require access to either a mobile phone or email account, as a PIN will be sent to you. Alternatively, you will need access to SystmOnline to accept or reject a share request sent to your account by the organisation wishing to view your record. *Please contact your GP if you are not enabled for SystmOnline.*

- **Custom lists** - You can put together your own custom lists for access, adding organisations to each of 3 lists i.e. does not require a security code (allowed list), requires a security code (verification list) and cannot access (prohibited list). The functionality for each list will act as described above, but it is you who can determine the level of access, which applies to them. This should be done in conjunction with your GP to ensure you understand the full implications of your decisions.

- **Dissent/Refusal of your permission** - You can refuse your permission for your record to become available to <u>all</u> NHS commissioned services and local authorities providing health services, using the clinical record computer system, SystmOne, which prevents us sharing your clinical record to any other organisation involved in your care. *Please carefully consider the benefits of sharing your record before choosing this option.*

- **Marking items as private** – If you have had a consultation about a particularly sensitive matter, you can ask for this section of your record to be marked as private. That way, even if you consent for another service to see your record, that consultation will not be shown outside the organisation that recorded it.

You can make changes to the above* at any time by contacting us or by logging onto your SystmOnline account. (*you cannot add an organisation to the prohibited list yourself, you must speak with your GP first if you wish to do this.)

6. Available audits

Audits are useful for your understanding about the types of organisation and individual(s) who are viewing your record. They allow you to raise any concerns about potential illegitimate or unnecessary access of your personal data with the relevant person or organisation. The ability to audit record access is a significant benefit of electronic records over paper records as it allows for a visible trail to be available to you in the following ways:

- **Alerts** - You can opt to receive an alert via SMS or email every time an individual at any health and social care organisation attempts to record your consent to view your record. This means that you can be confident that the appropriate people are viewing your record and you can raise concerns with any organisation where you feel this is not the case.

- **SystmOnline Record Audit** – You can view which organisations have accessed your electronic health record within SystmOnline. Ability to access this audit in SystmOnline is controlled by your GP. Any concerns about access can be raised with the relevant organisation.

- **Record Sharing List** – You can ask your GP practice to show you a list of all health and social care organisations currently caring for you and whether they have recorded your consent or dissent to view your record. If you disagree with the consent options recorded then you, or your GP, should contact those organisations and ask them to amend the setting.

7. Legal basis for holding and processing personal data

- Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member state law or a contract with a health professional. (Article 9(2)h of GDPR)

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. (Article 9(2)i of GDPR)

8. Contact details for our Data Protection Officer

- Bevan Healthcare CIC's Data Protection Officer is **Colin Gornall**
- Address: 14-16 Piccadilly, Bradford, BD1 3LS
- Telephone: 01274 322400

9. Data retention periods

The Data Protection Act 1998 (DPA) requires that we retain personal data no longer than is necessary for the purpose we obtained it for. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant. The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

It means that we will need to:

- review the length of time we keep personal data
- consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it
- securely delete information that is no longer needed for this purpose or these purposes
- update archive or securely delete information if it goes out of date.

Personal data will need to be retained for longer in some cases than in others. How long we retain different categories of personal data should be based on individual business needs. A judgement must be made about:

- the current and future value of the information
- the costs, risks and liabilities associated with retaining the information
- the ease or difficulty of making sure it remains accurate and up to date.

The appropriate retention period is also surrounding circumstances, any legal or regulatory requirements or agreed industry practice. At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it.

10. Data subject rights

You (the patient) are the data subject in this context.

- **The Right to Data Portability**

This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the 'midata' and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

- **Right of Erasure**

  The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing. *GP practices and other healthcare providers are EXEMPT form this.*

- **Right of Rectification**

  Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

- **Right of Access**

  Under the General Data Protection Regulation (GDPR), individuals will have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information. These are similar to existing subject access rights under the DPA. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

- **Right to Restrict Processing**

  Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

- **Right to be Informed**

  The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

- **Right to Object**

  Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/ historical research and statistics.

- **Rights Related to Automated Decision Making and Profiling**

  The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

11. **Objections, Concerns or Complaints**
    If you are happy for your data to be extracted and used for the purposes described in this notice then you do not need to do anything.

Should you have any concerns about how your information is managed at the practice, please contact Beth Kirby. If you are still unhappy following a review by the GP practice, you can then complain to the Information Commissioners Office (ICO) via their website **www.ico.org.uk**, casework@ico.org.uk, telephone: 0303 123 1113 (local rate) or 01625 545 745

12. Further information

- www.tpp-uk.com
- www.ico.org.uk
- https://portal.yhcs.org.uk/web/information-governance-portal/gp-igt-guidance?_20_folderId=12147008&_20_displayStyle=descriptive&_20_viewEntries=1&_20_viewFolders=1&_20_struts_action=%2Fdocument_library%2Fview&p_p_id=20&p_p_lifecycle=0&_20_entryStart=0&_20_entryEnd=20&_20_folderStart=0&_20_folderEnd=20&_20_action=browseFolder
- https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance