NHS
Cheshire and Merseyside

Privacy Notice
for Direct Patient Care
Empower
Amity – Patient Engagement Platform (PEP)

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services.

Cheshire and Merseyside Digital and Data Programmes

The programme was established to provide individuals in the Cheshire and Merseyside health & social care system with a digital portal which allows them to: access their own healthcare records; capture, record and share content with clinicians and wider support networks; access materials and support related to the self-management of their own health, wellbeing, and conditions; interact with healthcare services and wider support networks.

What is Amity?

The Amity Portal is an easy to use, web-based Patient Engagement Portal (PEP) and will help Empower individuals within the Cheshire and Merseyside region to manage their own health and wellbeing in one place. Amity will allow users access (via NHS Login) to view their GP medical records, GP appointments, digitised letters, questionnaires and resources. It will also suggest accredited resource apps to assist in self-care for their conditions.

Patients can view resources which are recommended by their clinical care team, and complete questionnaires which have been created and sent to them by their NHS provider. Patients can create their own circle of care, through which they can communicate with friends, family, carers, but also members of their clinical care team if they are signed up to Amity.

Amity core functionality for patients

- NHS login/authentication process
- Securely view digitised hospital letters
- Access to GP medical records
- View personalised health information and resources including
- recommended apps library
- Access a range of trackers for monitoring sleep, mood, pain,
- weight and more
- Create a virtual support network of family, friends, or carers
- Questionnaire builder and response capability
- Platform personalisation through onboarding journey

Our contact details

Name: NHS Cheshire and Mersey Integrated Care Board (ICB)

Amity – Patient Engagement Platform (PEP) has various functionality, each component has several different data controllers.

Data Controller: A controller decides on why and how information is used and shared.

View GP Practice record and View and book GP appointments and order repeat prescriptions

- The user's GP practice is the controller of the source data.
- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to access the source data via Amity and is therefore the controller in this regard.

View letters and correspondence

- Healthcare providers, typically NHS hospital Trusts, are the controllers of the source data.
- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to access the source data via Amity and is therefore the controller in this regard.

Secondary Care clinical records

- Healthcare providers, typically NHS Trusts and General Practices, are the controllers of the source data.
- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to access the source data via Amity and is therefore the controller in this regard.

Capture, record and share personal health record content with clinicians and support networks and Messaging

- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to be able to record and share their own data via the Amity platform.

Access materials and support

- Healthcare providers, typically NHS Trusts, are the controllers of the source data for the individual patients referenced above
- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to access the source data via Amity and is therefore the controller in this regard.

Interact with healthcare services and wider support networks - Questionnaires

- Healthcare providers, typically NHS Trusts, are the controllers of the data relating to a request for a questionnaire to be issued, and the questionnaire responses received back.
- NHS Cheshire and Merseyside exercises overall control over the purposes and means of the processing of personal data required for patients to use this functionality via Amity and is therefore the controller in this regard.

Access and security controls

- NHS England for any NHS Login related processing.
- NHS Cheshire and Merseyside for other Amity logins.

In addition, the C&M ICB Privacy Notice can be found at: **Privacy Notice** - NHS Cheshire and Merseyside

The Amity – Patient Engagement Platform (PEP) email address is: Amity@imerseyside.nhs.uk

Other Associated Documents

This Privacy Notice is part of the **Data Sharing Agreement Tiered Framework** and should be read in conjunction with the three associated Tier documents:

- Tier Zero Memorandum of Understanding
- Tier One Data Sharing Agreement – Standards
- Tier Two Data Sharing Agreement - Workstream: Unified Direct Care

General inquiries email address: Amity@imerseyside.nhs.uk

Data Controller(s) is/are:

- NHS Cheshire and Merseyside ICB
- NHS England
- NHS Healthcare providers across Cheshire and Merseyside
  - General Practices
  - NHS hospital Trusts

Name: NHS Cheshire and Merseyside ICB

Address: NHS Cheshire and Merseyside, Regatta Place, Brunswick Business Park, Summers Lane, Liverpool, L3 4BL

Phone number: General enquiries - NHS Cheshire and Merseyside – direct general enquiries to your local Place team (within this link)

Email: enquiries@cheshireandmerseyside.nhs.uk

Data Protection Officer: mlcsu.dpo@nhs.net

Website: https://www.cheshireandmerseyside.nhs.uk/

Name: NHS England

Address: NHS England, PO Box 16738, Redditch, B97 9PT

Phone number: 0300 311 22 33

Email: england.contactus@nhs.net

Website: https://www.england.nhs.uk/

Name: NHS Healthcare Providers – General Practice and Hospital Trusts
Please look up details for your NHS Healthcare Provider here:

General Practice: Find a GP - NHS (www.nhs.uk)

NHS Provider Trusts: NHS England » NHS provider directory

How do we get information and why do we have it?

The personal information we collect is provided directly from you because:

- You have provided information to your NHS healthcare provider – this is used directly for your care, and also to manage the services we provide, for approved research, to clinically audit our services, investigate complaints, or to be used as evidence as part of an investigation into care.

We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing.

What information do we collect?

Personal information

We currently collect and use the following personal information:

- Name
- Date of Birth
- NHS Number
- Identification Number (e.g. Hospital Number)
- Online identifier (e.g. Email Address, IP Address)

Please note, the identifiable data is not used unless a) it is for direct care; or b) the patient has consented.

The Amity PEP involves the processing of personal information and large-scale use of special category data. It therefore requires a Data Protection Impact Assessment (DPIA).

Amity (https://amitywellness.co.uk/) is a web-based Patient Engagement Platform (PEP) designed to provide individuals, patients, carers, and clinical staff with a digital platform to empower individuals to care for themselves and take control of their own health and wellbeing.

The key aim of the programme is to provide individuals of the Cheshire and Merseyside region with a digital portal which allows them to:

- access their own healthcare record(s);
- capture, record and share content with clinicians and wider support networks.
- access materials and support related to the self-management of their own health, wellbeing, and conditions.
- interact with healthcare services and wider support networks.

NHS organisations across Cheshire and Merseyside came together to develop and provide this functionality. Under the original framework of the Cheshire and Merseyside Health and Care Partnership, and later the Integrated Care System (ICS), and the associated Digital Strategy, organisations are working together to – ultimately - provide a joined-up digital experience for patients which aligns with the region's ambitions for integrated, place-based care.

More sensitive information

We process the following more sensitive data (special category data):

- Data concerning physical or mental, which may include:
    - clinical diagnosis and history
    - medications
    - clinic letters
    - any other pertinent health data for direct patient care.
- Data revealing racial or ethnic origin
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- Biometric data (where used for identification purposes)
- Data revealing religious or philosophical beliefs

Patient data and confidential patient information

Confidential patient information is information that both identifies the patient and includes some information about their medical condition or treatment.

Further information about the NHS and Confidential patient information can be found here.

Who do we share information with?

We may share information with the following types of organisations:

- Amity (via direct link (Application Programming Interface (API) to a platform which surfaces GP held clinical records (Evergreen platform used as a proof of concept) shares GP clinical record information only with the patient to which it relates.
- Amity only shares the data which describes an association between a user (patient) and a clinical / care resource with the user themself.
- Amity shares correspondence only with the patient to which it relates.
- Amity also sends information back to the healthcare provider's via a Third Party Supplier (Synertec used as a proof of concept) to help providers manage their responsibilities around the delivery of correspondence.
- Third party data processors (such as IT systems suppliers)
- Users can individually choose to share their information with other Amity users in order to further support themselves.
- Amity only shares the data which describes an association between a user (patient) and a clinical / care resource with the user themself.
- Users receive and complete questionnaires via Amity and share their responses with the healthcare provider which issued the questionnaire. It is made available to the healthcare provider via three mechanisms: (i) the clinician is a member of the patient's 'circle' so is able to view the information within the Amity platform; (ii) the Trust can choose to download the information, from the Amity platform, in PDF document format; (iii) the Trust can choose to extract the information, from the Amity platform, in CSV file format.
- Information received back from patients will be stored within the Trust EPR.
- Messages are shared with the other Amity user(s) that the sending user has opted to share their information with.
- NHS Login user credentials are shared with other NHS Login 'connected services'.

In some circumstances we are legally obliged to share information. This includes:

- When required by NHS Digital - the organisation which develops national IT and data services
- When registering births and deaths
- When reporting some infectious diseases
- When a court orders us to do so
- Where a public inquiry requires the information

We will also share information if the public good outweighs your right to confidentiality. This could include:

- Where a serious crime has been committed
- Where there are serious risks to the public or staff
- To protect children or vulnerable adults

We may also process your information in order to de-identify it, so that it can be used for purposes beyond your individual care whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

Is information transferred outside the UK?

No, we do not transfer your information outside the UK.

What is our legal basis for using information?

Personal information

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal information is:

GDPR 'processing of personal data' is met by Article 6(1)(e)

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

See **Annex 1** for the most likely laws that apply when using and sharing information in health and care.

More sensitive data

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using more sensitive (special category) data is:

GDPR 'processing of special category data' is met by Article 9(2)(h)

- Processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the individual, medical diagnosis, the provision of health or social care or treatment or the management of health or social care services, with appropriate safeguards.

See **Annex 1** for the most likely laws that apply when using and sharing information in health and care.

Common law duty of confidentiality

We have to satisfy the common law duty of confidentiality when using health and care information.

In our use of health and care information, we satisfy the Common Law Duty of Confidentiality (CLDC) which is addressed by implied consent for direct care purposes.

Explicit consent applies where individual Amity users (i.e. – patients / individuals) provide their own information. Amity provides a place for users to systematically capture and store their own healthcare related data and, if they choose, share it with others.

Individuals with capacity accept the Terms and Conditions and provide their valid, informed consent for a specific purpose without prejudice. See further details below.

The right to object under S21 of the UK General Data Protection Regulation, as enacted, is also relevant. Patients and service users have a right to object to their medical information being used in order to provide safe and effective care and have the right to register this objection in writing, or verbally, to the clinician concerned.

Other uses of your data are met by other UK legislation – please see Annex 1, which sets out the laws that health and care organisations rely on when using your information.

How do we store your personal information?

Your information is securely stored subject to local record retention policies, for the time periods specified in the Records Management Code of Practice 2021. We will then dispose of the information as recommended by the Records Management Code. We will securely dispose of your information, for example by shredding paper records, or wiping hard drives to legal standards of destruction.

What are your data protection rights?

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information (known as a subject access request).

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at Amity@imerseyside.nhs.uk if you wish to make a request.

Automated decision making

Amity does not undertake automated decision-making.

National data opt-out

The **National Data Opt**-out does not apply for direct care. However, in the Data Sharing Agreement **Type 1 Opt-outs** (those who do not want their information shared outside of General Practice for purposes other than direct care) will be upheld.

The information collected about you when you use health and care services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this when allowed by law.

Most of the time, the data used for research and planning is anonymised, so that you cannot be identified and your confidential patient information is not accessed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters.

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

How do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at Amity@imerseyside.nhs.uk

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Annex 1

The laws that health and care organisations rely on when using your information

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example, if an organisation is sharing information because they are required by law to do so, they need to identify which law is requiring this. The following are the most likely laws that apply when using and sharing information in health and care. This list is not exhaustive.

Abortion Act 1967 and Abortion Regulations 1991

Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.

Access to Health Records Act 1990

Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.

Care Act 2014

Defines how NHS organisations and local authorities must provide care and support to individuals, including for the management of safeguarding issues. This includes using information to assess any person who appears to require care and support.

Children Act 1989

Sets out the duties of local authorities and voluntary organisations in relation to the protection and care of children. It requires organisations that come into contact with children to cooperate and share information to safeguard children at risk of significant harm.

Control of Patient Information Regulations 2002 (COPI)

Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such measles or COVID-19. It also allows for information to be shared where approval has been given for research or by the Secretary of State for Health and Social Care.

Coroners and Justice Act 2009

Sets out that health and care organisations must pass on information to coroners in England.

Employment Rights Act 1996

Sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

Equality Act 2010

Protects people from discrimination based on their age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex, sexual orientation. Organisations may need to use this information to ensure that they are complying with their responsibilities under this Act.

Female Genital Mutilation Act 2003

Requires health and care professionals to report known cases of female genital mutilation to the police.

Fraud Act 2006

Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.

Health and Social Care Act 2008 and 2012

Sets out the structure of the health and social care system and describes the roles of different types of organisations. It sets out what they can and can't do and how they can or can't use information. It includes a duty for health and care staff to share information for individual care, unless health and organisations have a reasonable belief that you would object. In addition, health and care organisations may need to provide information to:

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England
- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care
- NHS Digital, which is the national provider of information, data and IT systems for health and social care.

Health and Social Care (Community Health and Standards) Act 2003

Allows those responsible for planning health and care services to investigate complaints about health and care organisations they have a contract with.

Health Protection (Notification) Regulations 2010)

Requires health professionals to help manage the outbreaks of infection by reporting certain contagious diseases to local authorities and to the UK Health Security Agency. The UK Health Security Agency is responsible for protecting people from the impact of infectious diseases.

Human Fertilisation and Embryology Act 1990

Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.

Human Tissue Act 2004

Requires health organisations to report information about transplants, including adverse reactions to the Human Tissue Authority.

Inquiries Act 2005

Sets out requirements in relation to Public Inquiries, such as the UK COVID-19 Inquiry. Public Inquiries can request information from organisations to help them to complete their inquiry.

Local Government Act 1972

Sets out the responsibilities of local authorities in relation to social care including managing care records appropriately. For example, it lays out how they should be created, stored and how long they should be kept for.

NHS Act 2006

Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These include a limited number of approved research and planning purposes. Information can only be used where it is not possible to use information which doesn't identify you, or were seeking your explicit consent to use the information is not practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958

Defines all records created by the NHS or local authorities as public records. This includes where organisations create records on behalf of the NHS or local authorities These records therefore need to be kept for certain periods of time, including permanently in some cases.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

Requires employers to report deaths, major injuries and accidents to the Health and Safety Executive, the national regulator for workplace health and safety.

Safeguarding Vulnerable Groups Act 2006

Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.

Statistics and Registration Service Act 2007

Allows health organisations that plan services and local authorities to receive and disclose health and care information to the Office for National Statistics (ONS). The ONS is the UK's largest independent producer of official statistics.

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011

Requires any person to share information with the police for the prevention and detection of terrorism related crimes.

The Road Traffic Act 1988

Requires any person to provide information to the police when requested to help identify a driver alleged to have committed.