Privacy Notice (under review)

Northern Ireland Electronic Care Record (NIECR)

Your Information – How we use it

The Northern Ireland Electronic Care Record (NIECR) is a computer system which has been in operation for the since 2013 which allows care professionals such as Doctors, Nurses, and Social Workers, as well as certain authorised administrative staff, to get important information about their patients' medical and social care history.

The information that is stored in your record includes;

- Personal data such as your address, date of birth
- Medicines
- Allergies
- Illnesses e.g. diabetes, heart conditions
- Treatments you are receiving
- Laboratory and radiology results

This information will be looked at by Health and Social Care (HSC) professionals. Staff may share information with each other about their patients; however all staff are obliged, within their contracts of employment, within their professional Codes of Conduct and by the common law **Duty of Confidentiality** to ensure that all personal information is treated with the highest possible levels of confidentiality**.** . Please refer to section 'Sharing information about you and your care' for more detail. Patient information that is collected and displayed in NIECR is respected and we have security measures in place to protect it.

Changes to sharing your health record on NIECR

There has been a significant change in the legislation in how we hold and process your health care information**.** As a result of this change, and in order to provide you with the best care or service, your NIECR record may need to be shared with authorised individuals directly involved in your health and social care**.**

In summary, staff will use NIECR to provide you with safe and effective care. Staff will access information such as blood tests, radiology reports, diagnoses, and treatment that is recorded across the region to provide you with continuity of care. We will ensure that this is in accordance with the General Data Protection Regulations and the Data Protection Act, and that staff adhere to their contractual

obligations and to the common law duty of confidentiality. See Laws Used to Process Your Information for the relevant legislation links.

The laws used to process and protect your information

The Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK defines a legal basis for us to take steps to ensure that personal data is adequately protected by placing a legal obligation on us to do so. This legislation provides us with a framework to ensure that your information is handled securely and gives us a legal basis for using this information for your care.

In order to comply with our obligations under the GDPR and DPA, any personal data 'processing' carried out by HSCNI must have lawful basis (Art 6 GDPR) and, as the processing relates to data concerning health, must also comply with a lawful processing condition (Art 9 GDPR), as further defined by the DPA 2018.

Lawful processing basis - the 'public task' basis has been determined to be the most relevant lawful basis. This is detailed in Article 6 (i) (e) of GDPR and Section 8 of the Data Protection Act.;

> *GDPR 6 (1). Processing shall be lawful only if and to the extent that at least one of the following applies: (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…"*
>
> *Section 8 – DPA "In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for…(c)the exercise of a function conferred on a person by an enactment or rule of law; (d)the exercise of a function of the Crown, a Minister of the Crown or a government department…"*

Lawful processing condition – Article 9 (1) of the GDPR prohibits the processing of certain sensitive personal data, including data concerning health. The exemption from this prohibition on processing special category data as set out in GDPR Article 9 (2) (h) i.e.

> *9 (2). Paragraph 1 shall not apply if one of the following applies:*
>
> *(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,*

medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

9 (3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

This is further defined and detailed in DPA Section 10 and DPA Schedule 1 Part 1.

We are also obliged to comply with the following law and professional guidance;

Health and Social Care (Reform)Act (Northern Ireland) 2009

Department of Health Code of Practice on Protecting the Confidentiality of Service User Information
https://www.health-ni.gov.uk/sites/default/files/publications/health/user-info-code2019.pdf

GMC guidance on patient confidentiality

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/using-and-disclosing-patient-information-for-direct-care

Why we process it

Processing is any operation performed on personal data, and includes collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, disclosure, dissemination, restriction, erasure or destruction.

We use your information to -

- Guide – it helps us assess your needs and make decisions with you
- Record the care you receive - referrals, appointments and services
- Review and support carers – If you care for someone, it may be necessary to review your NIECR information to assess additional support for you or the people you care for.
- Give us up-to-date information - helping us to provide better care

- Provide faster care – sharing information on NIECR means we can help you quicker
- Improve Services - we do on occasions safely share data in a way that does not identify the individual patient. . This is called anonymised information and can be used for planning, research and audit purposes – this helps us make best use of resources, supporting prevention of ill health and improving treatment. We anonymise your information prior to sharing.
- Train and educate staff – we review our patient care to ensure good practice across the services we offer you.
- Review deaths - multidisciplinary mortality reviews; deaths that occur in HSC Trusts are subject to review. This includes the multidisciplinary team providing the direct patient care reviewing the treatment and care provided and acting upon any learning lessons identified. This improves the quality of care for patients as well as patient safety.

Storing your information

Patients' information is currently stored in line with Department of Health Good Management Good Records Guidelines Disposal Schedule. The precise retention period for any particular type of record will vary depending on the nature of the information

Links to the retention and disposal schedules:

https://www.health-ni.gov.uk/articles/disposal-schedule-section-g-part-1

https://www.health-ni.gov.uk/articles/disposal-schedule-section-g-part-2

In some instances individuals have the right to ask for their personal information to be erased (the right to erasure). However the right of erasure does not apply for information held within the NIECR system. Article 17(3)(c) of GDPR states that the right to erasure …"shall not apply …. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3)."

How information is used to help you

Storing data on the system means -

- Your information is kept accurate and up to date
- Your information is available when you need to attend another hospital in an emergency which may prevent repeat tests

- We can decide on the medical priorities for referrals quicker and assign urgent appointments faster
- We provide the best possible care and you receive the right treatment.

How information is used to help us

Your information is used by staff to have your summary details on screen quickly and to easily access your patient record when needed. This enables staff to view services you have received, tests you have had carried out and appointments you have attended.

Your information is used for processing and reporting on behalf of the Health Trusts. This can help us to assess how we can deliver better services to our patients.

Sharing information about you and your care

Your information will be shared with professionals in:

- Family practitioner services incl. general practice
- Acute services in hospital
- Outpatient services in hospital
- Community services such as Social Care
- Community based optometry

This will include people such as:

- GPs
- Doctors
- Nurses
- Social workers
- Optometrists
- Pharmacists
- Clinical Administration

Access is based on role type so the information available to each of these users will depend on their access level. Safeguards are in place to enable staff to access summary information about a patient when it is relevant to their job and appropriate to do so. Staff only access records with a clinical need.

When we refer to role type we mean for example a consultant will have full access to the relevant patient information on NIECR. So a Cardiology consultant (a doctor with a specialism in dealing with patients who have heart conditions) will have access to all of a patient's medical records in order to build up a complete picture of their

patient's health, this is to provide the best possible care for that patient. Whereas an administration role would have NIECR access limited to only viewing information related to their role such as referral letter lists and outcomes which help them to book further patient appointments, or blood results in order to be able to give patients their blood results if appropriate. Staff are trained and have a legal duty to keep your information safe and confidential.

The software supplier for NIECR provides the technical support to ensure the system is working effectively. Your information will only be shared to resolve technical errors or issues following secure protocols in line with applicable organisational policies. Should personal data be necessary to resolve an issue, this will be minimal information required.

We only share information when absolutely necessary. We have procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Should NIECR receive requests for information from external bodies each will be considered on an individual basis; if approved your information will only be accessed with your consent, an example of this would be a request by Independent Health Care Providers.

Information shared by law

There may be occasions when where your information can be shared with other organisations without you consent, but this will only happen when it is;

- Required by law or by a court order
- Necessary to detect or prevent a crime, including allegations or suspicions of fraud
- Necessary to protect the public from serious harm e.g. the protection of vulnerable adults
- Required for monitoring certain health conditions e.g. infectious diseases.

Security of your information

- All staff are required to complete information governance training regularly
- Governance policies and procedures are in place; these are available on all of the Health Trusts' websites.
- All staff within HSC who access NIECR have appropriate access levels for their role, not everyone who has access to the system can view your personal information. This is known as controlled access.

- A record is kept every time a member of staff accesses your information. Regular checks and audits are carried out on this this activity to ensure that only authorised staff are accessing personal information.
- There are security measures put in place to ensure a high standard of IT security across all Health and Social Care Services protecting them from all threats. These could be internal, external, deliberate or accidental threats.

How do I see my information?

You have a right under data protection legislation to obtain a copy of information held about you. If you want to see the information held about you, or ask about how we use it, we would suggest as a first step an informal approach to your GP or other HSC professional that you may be seeing.

To formally request access to your NIECR, or any health and care record (a Subject Access Request) you need to write or speak to your GP Practice or the Health and Social Care Trust where you are receiving or have received care. In most cases, the deadline for response will be one calendar month, although this can be extended to 3 months where a request is deemed 'complex'.

Enquiries

If you would like to know more about how we use your information and your rights please contact our Privacy Officer.

Email: NIECRPrivacy.Officer@hscni.net

Phone: You can telephone **0300 555 0205** for information
(Option 1: NIECR information, Option 3: How your information is used)

Further Information

If you have any further concerns or queries on how your personal data is being processed you can contact the **Information Commissioners Office.**

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

Tel: **0303 123 1113**
https://ico.org.uk/global/contact-us/