



NIPACS+

Privacy Notice

Version 1.0
June 2024

Document History

Document Location *This document is only valid on the day it was printed and the electronic version is located on the Programme SharePoint site.*

Versions			
Version	Date	Change Made	Author
1.0	February 2024		Ryan McLaughlin

Approved By	Date
J Allison	June 2024

Table of Contents

Document Location *This document is only valid on the day it was printed and the electronic version is located on the Programme SharePoint site.* 2

1. What is NIPACS+?

The NIPACS+ Programme ('NIPACS+') is a single regional enterprise imaging solution for Northern Ireland. It consists of a Radiology Information System (RIS), Picture Archiving and Communication System (PACS) and Vendor Neutral Archive (VNA):

RIS manages the patient pathway through Radiology.

PACS is a system providing the distribution and display of medical imaging.

VNA is a medical imaging technology in which images and documents (and potentially any file of clinical relevance) are stored (archived) in their native format with a standard interface, such that they can be accessed in a vendor-neutral manner by other systems.

NIPACS+ will also provide storage for imaging from other specialties such as cardiology, endoscopy, ophthalmology, and others. This will replace the multiple individual image storage systems for these specialities already in existence.

NIPACS+ will provide reporting functionality for Radiology and Digital Pathology. It will also include a research database and teaching file functionality.

A summary of NIPACS+'s objectives is outlined below.

- To improve patient safety and ensure that appropriate digital imaging services are available where and when required to support effective and efficient care delivery.
- Sustain and enhance this critical service.
- Deliver a once for Health and Social Care Northern Ireland (HSC) approach to RIS/PACS/VNA.
- To enable effective clinical pathways and other ongoing HSC transformation initiatives.
- To standardise on best practice across HSC to ensure a consistent and high-quality imaging service.

2. The Laws used to process and protect your information

- the United Kingdom General Data Protection Regulation (UK GDPR),
- the Data Protection Act 2018 (DPA 2018) to the extent that it relates to processing of personal data and privacy,
- all other applicable Law about the processing of personal data and privacy.

3. Who can access my information?

Only those involved in providing or supporting your care can access your information. Your information will not be shared with anyone else unless there is a clear legal basis for doing so.

4. Who is involved in my care?

Pursuant to Article 13 of the UK GDPR the Data Controllers of the Personal Data are as follows:

- Northern Health and Social Care Trust,
- Belfast Health and Social Care Trust,
- Southern Health and Social Care Trust,
- South Eastern Health and Social Care Trust South Eastern Health and Social Care Trust
- Western Health and Social Care Trust,
- The GP Practices operating in Northern Ireland,
- Other Third-Party Providers contracted by the Trusts to provide patient care.

In line with their statutory functions as set out within Article 15 of the Health and Social Care (Reform) Act (Northern Ireland) 2009, the Business Services Organisation (BSO) will provide some support functions to the above (such as hosting NIPACS+) but will not be directly involved in patient care or clinical decisions and will not access personal data other than to provide this support function. The BSO is therefore noted as a data processor for NIPACS+.

5. Storing your information

The personal data will be processed in line with the Northern Ireland 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/sites/default/files/publications/health/gmgr-disposal-schedule.pdf>

6. Nature and purposes of Processing

Personal Data will be processed for the purposes detailed below:

Clinical Decision Making – Images will be analysed by the controllers for the purposes of clinical diagnosis and decision making.

Storage – data will be stored in BSO's regional data centre and/or at any or all of the Trust sites to enable the data controllers to plan, manage and deliver services. The hardware and software will be managed by the Supplier.

Alteration – data will be migrated by the Supplier from the incumbent supplier solutions to the NIPACS+ Solution to enable continuity of service for controllers and maintain the established benefit of image sharing.

Disclosure by transmission and retrieval – data will be accessed for the purpose of NIPACS+ solution fault or error correction. Performance monitoring and resolution will be carried out by the Supplier.

Recording – Voice files and profiles will be obtained from NIPACS+ users, stored and analysed to facilitate user specific voice recognition text input. The Personal Data will not be processed in an automatic way (including in the form of profiling).

Artificial Intelligence – NIPACS+ will use a cloud-based, software-only device designed to host and manage the launch of third-party applications that process patient data, such as medical images and associated reports. It facilitates the transfer of relevant pseudo anonymised data to the appropriate third-party application for processing and subsequently returns the generated results. All third-party applications are hosted within the platform's infrastructure environment. Hence, no patient data is sent outside the platform for processing.

The Data Controllers process personal data for the purposes of public task, legal obligation, provision of healthcare - management of HSC systems, ensuring high standards of quality and safety of healthcare systems and/or scientific or historical research purposes compliant with Article 6(1)(e), 6(1)(c), 9(2)(h), 9(2)(i) and 9(2)(j) of the UK GDPR. Acting on instruction, the BSO also processes (i.e. stores) data under the same provisions.

Information shared by law -There may be occasions where your information can be shared with other organisations, but this will only happen in very specific circumstances. This may include (but is not limited to) data:

- required by law or by a court order.
 - necessary to meet the requirements of Section 66 of the Children (Northern Ireland Order (1995).
 - 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;
- or
- required for monitoring certain health conditions e.g., infectious diseases.

7. Your Personal information

In addition to your demographic information (name, DOB, address, GP, etc) NIPACS+ will store available images from all diagnostic examinations performed on you at any of the Health and Social Care (HSC) Trust sites. It also stores imaging reports for these examinations' information collected is outlined in Appendix 2.

The NIPACS+ Solution transmits dose report data outside of the HSC network to a system called DoseTrack. The dose data is transmitted with all patient identifiers and demographics

removed at the point of the data leaving the HSC network. The data is encrypted via HTTPS with EC DS certificates and stored on a secure private server hosted in the Microsoft Azure cloud. The data centre is secured by firewall rules to only allow point-to-point access from the NIPACS+ Solution, which stops any access from other sources. Information can be viewed by HSC professionals. Such 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, the Code of Conduct for HSC employees, data protection legislation and by the common law Duty of Confidentiality to ensure that all personal information is treated with the highest possible levels of confidentiality. Personal data will only be shared by and to those staff who require sight of it to perform their duties.

Personal data may also be processed by Independent Health Sector professional staff. Such staff will also be bound by contractual arrangement, data protection legislation and common law duty of confidentiality.

8. What are my Rights?

Individuals have certain rights under UK GDPR, namely:

- The right to obtain confirmation that their personal data is being processed, and access to personal data,
- The right to have personal data rectified if it is inaccurate or incomplete,
- The right to have personal data erased and to prevent processing, in specific circumstances,
- The right to 'block' or suppress processing of personal data, in specific circumstances,
- The right to portability, in specific circumstances,
- The right to object to the processing, in specific circumstances,
- Rights in relation to automated decision making and profiling.
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

Detailed guidance on your rights is available from the Information Commissioner's Office:

<https://ico.org.uk/for-the-public/>

9. Data Sharing

The sharing of Personal Data during the term of the NIPACS+ Solution is required for the Joint Controllers and data processors to perform their duties.

The scope of data shared shall be restricted to the required minimum. The collected data will not be used for any other purposes than those specified in Section 7 as required for the NIPACS+ Solution. The Joint Controllers may process the data for other legitimate purposes. Where this is applicable, the Joint Controllers will provide detail of this additional processing via further privacy notices or other suitable communications.

Data subjects may contact the data controllers in relation to personal data processing and the exercise of rights related to personal data processing. Only Trusts have sufficient system access to provide this information following receipt of a subject access request (SAR). Contact details of the Trusts are set out within Appendix 1.

10. Security of your information

All staff are required to complete information governance training regularly. Information Governance policies and procedures are in place.

Access to NIPACS+ will be strictly controlled. Access will also be restricted to only those staff who require it for the discharge of their duties.

An audit record of all activity within NIPACS+ will be maintained within the NIPACS+ solution. Access to audits are available to authorised users.

There are 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.

11. How can I access my information?

Access to information

The UK GDPR gives individuals the right to access information that NIPACS+ holds about them by submitting a Subject Access Request (SAR) to the data controller(s).

Freedom of Information

The Freedom of Information Act 2000 provides any person with the right to obtain information held by NIPACS+, subject to a number of exemptions.

Making a request

Please contact your individual Trust area who can provide more detail on how to submit a request. Contact details are provided in Appendix 1. Data Protection Officers (DPOs) may also be contacted through the details provided in Appendix 1.

12. Changes to our privacy notice

NIPACS+ will keep this privacy notice under regular review.

Appendix 1

Trust Information Governance Contact Details

Northern Trust

Information Governance Department
Route Complex, 8e Coleraine Road, Ballymoney, Co. Antrim, BT53 6BP
Telephone: 028 276 61293
Email: info.governance@northerntrust.hscni.net

Southern Trust

Information Governance Office
Ferndale, Bannvale House, 10 Moyallen Road, Gilford, BT63 5JY
Telephone: 028 37561458 / 028 37565743
Email: Foi.Team@southerntrust.hscni.net

Western Trust

Information Governance Office; Tyrone & Fermanagh Hospital;
1 Donaghane Road; Omagh; Co. Tyrone; BT79 0NS
Telephone: 028 8283 5440
Email: Information.Governance@westerntrust.hscni.net

South Eastern Trust

Information Governance Dept
Lough House, Ards Hospital, Newtownards, BT23 4AS
Telephone: 028 9151 2210
Email: informationgovernance@setrust.hscni.net

Belfast Trust

Data Protection Office, Belfast Health & Social Care Trust
1st Floor Admin Building, Knockbracken Healthcare Park, Saintfield Road, Belfast, BT8
8BH
Telephone: 028 9504 6955
Email: dataprotection@belfasttrust.hscni.net

Appendix 2

Categories of Data Subject

- Staff (including volunteers, agents, and temporary workers)
- Service Users
- Carers

6.1.1 Service Users

- Health and Care Number (HCN)
- Date of birth
- Name – Surname, Forename, Preferred Name
- Title
- GP
- Address – residential address and any alternative correspondence address
- Phone Number
- Gender
- Height and Weight
- Date of Last menstrual period and reason for override (e.g. use of contraceptive)
- Alerts - including, but not restricted to, allergies, MRI contraindications, contrast reactions,
- All Referrals (including cancelled and rejected) –clinical history, reason for referral, referral source, referrer and referring clinician, priority, request category (inpatient, outpatient, GP, Emergency Department), authorising signature and examination protocols,
- Free text referral notes – common notes include appointment notes, reasons for patient cancellations and Did Not Attend,
- Examination details – radiation dose, Operator name, date of exam, type of exam, medicines used as part of examination (including oral contrast, iv contrast, radioisotopes etc.),
- Image Report,
- Dose Information – see in section 7 for more information.

6.1.2 Staff

- Full name
- Job title
- Role
- Professional registration number for reporting staff
- Consolidated server account code
- Contact details (telephone, email, department)

6.1.3 Carer and Comforter

- Name
- Date of Birth
- Gender
- Pregnancy Status
- Connection to Service User