Privacy Notice

YOUR DATA, YOUR RIGHTS: NERHA'S PRIVACY NOTICE FOR PATIENTS, STAFF, AND SERVICE USERS

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

OUR CONTACT DETAILS

Name:	North-East Regional Health Authority
Address:	Offices 1,9, 34-38, Ocean Village Shopping Centre
	Ocho Rios P.O., St. Ann, Jamaica W.I
Contact:	1 (876) 974-4114 | 1 (876) 795-3107
Email:	**info@nerha.gov.**jm
Website:	www.nerha.gov.jm

We are the controller for your information. A controller decides on why and how information is used and shared.

DATA PROTECTION OFFICER CONTACT DETAILS

Our Data Protection Officer, Shavonae Johnson-Bent, is responsible for monitoring our compliance with data protection requirements. You can contact her with queries or concerns relating to the use of your personal data at data.protectnerha@nerha.gov.jm or 1 (876) 795-3107.

INTRODUCTION

This Privacy Notice outlines how the **North-East Regional Health Authority (NERHA)** collects, uses, shares, and protects your personal information, in accordance with applicable data protection laws, including the **Data Protection Act, 2020 (DPA)** and, where relevant, the **General Data Protection Regulation (GDPR)**.

We are committed to ensuring transparency in how we handle your personal and sensitive information and want you to feel informed and confident about your rights and our responsibilities.

This Privacy Notice is intended to help you understand:

- The types of personal and sensitive personal data we collect
- How that data is used, stored, shared, and processed
- The steps we take to safeguard your information
- Your rights and choices regarding your personal data

This notice applies to all individuals whose data is collected and processed by the NERHA, including **patients, employees, service users, visitors**, and **anyone who interacts with us**—whether in person, through our website, or by other means of communication.

Specifically, this Privacy Notice explains:

1. What personal and sensitive personal data we collect during your interactions with us
2. How that data is collected, used, shared, stored, and processed
3. The security measures in place to protect your data
4. Your rights and options regarding the management of your information
5. How to contact us to access, correct, or inquire about your data

We encourage you to read this notice carefully to understand how your personal data is handled and protected by the NERHA.

OUR COMMITMENT TO DATA PROTECTION

At the NERHA**,** we take your privacy seriously. Whether you are a patient, employee, visitor, or service user, we are committed to protecting your personal and sensitive information.

We respect your right to privacy and are guided by strict policies and legal standards, particularly the DPA. We take all reasonable steps to ensure the confidentiality, integrity, and security of the data you share with us.

Our commitment includes:

- Using your data only for appropriate and lawful purposes
- Keeping your data secure through strong safeguards
- Being transparent and accountable in how we handle your information
- Preventing unauthorised access, misuse, or data breaches

We value your trust and will always treat your personal information with care, professionalism, and in full compliance with the law.

HOW DO WE GET INFORMATION, AND WHY DO WE HAVE IT?

The personal information we collect is provided directly from you for one of the following reasons:

- You have provided information to receive care. This information is used directly for your treatment, to manage our services, conduct clinical audits, investigate complaints, or serve as evidence in care-related investigations.
- You have applied for funding for continuing healthcare or a personal health budget.
- You have applied for a job with us or are currently employed by us.
- You have joined our patient participation group.
- You have submitted a complaint.
- You have communicated with us through various means, including email, telephone, online forms, chat functions, newsletter sign-ups, contests, surveys, patient registration/bookings, event planning or participation, service requests, applications, recordings, or other interactions—either in person at one of our locations or electronically.

In addition to the personal information you provide directly, we may also indirectly receive personal information about you from third parties. This is done in accordance with applicable data protection laws and is essential for delivering safe, coordinated, and effective care, as well as fulfilling our legal and operational responsibilities.

We may receive your personal information from:

- **Other health and care providers or organisations involved in your care**, such as hospitals, clinics, laboratories, or community health services. This allows us to coordinate and continue your treatment effectively.
- **Family members, legal guardians, or carers**, who may share information necessary to support your care, wellbeing, or decision-making, especially where you are unable to provide that information yourself.
- **Regulatory or oversight bodies**, such as the Ministry of Health & Wellness (MOHW), in the context of audits, inspections, or compliance reporting.
- **Employers**, when information is required for occupational health purposes or pre-employment medical assessments.

- **Third-party service providers**, including laboratories, diagnostic services, insurers, or specialists to whom you have been referred or who are involved in your care or benefits processing.
- **Law enforcement or safeguarding agencies**, when disclosure is required by law or in the interest of public protection or safety.
- **Educational institutions or training bodies**, in cases where we supervise students or provide educational placements involving your care.

All indirectly received information is treated with the same level of confidentiality, security, and care as information you provide directly. It is used only for the purposes it was collected and in line with legal requirements.

WHAT INFORMATION DO WE COLLECT?

PERSONAL INFORMATION

We collect and use a variety of personal information to deliver healthcare and other related services, to fulfil our legal obligations, and to support our operational and administrative activities.

Personal information refers to any data that can be used to identify a living individual—directly or indirectly. This may include, but is not limited to:

- **Personal identifiers and contact information** (e.g., full name, home address, email address, telephone number, date of birth, gender, nationality)
- **Identification details** (e.g., driver's licence number, passport number)
- **Photographic identity** (e.g., photographs for staff ID badges, event participation, or internal communications)
- **Demographic information** (e.g., marital status, occupation)
- **Location data** (e.g., IP address or location tracking during service access)
- **Service-related information** (e.g., appointment history, services accessed, event participation)
- **Communication records** (e.g., inquiries, complaints, feedback, or requests made via phone, email, forms, or chat functions)
- **Multimedia records** (e.g., audio or video recordings from patient visits, events, or interviews)

MORE SENSITIVE INFORMATION (SPECIAL CATEGORY DATA)

Under the DPA and the GDPR, certain types of personal information are considered particularly sensitive and are afforded additional protections. These include data relating to an individual’s health, ethnicity, religion, and more.

We process the following special category (sensitive) data where necessary and in accordance with legal requirements:

- **Health and medical information** (e.g., details about your physical or mental health, diagnosis, treatment plans, medical history, appointment records)
- **Data revealing racial or ethnic origin**
- **Data concerning a person’s sex life or sexual orientation** (only when clinically relevant or required for care or safeguarding)
- **Genetic data** (e.g., DNA or other genetic markers collected as part of a medical diagnosis or treatment)
- **Biometric data used for identification purposes** (e.g., signature, fingerprint or facial recognition systems, if applicable)
- **Religious or philosophical beliefs** (only when relevant to care delivery, such as dietary or cultural preferences)
- **Trade union membership** (only if disclosed in employment-related interactions)

- **Information relating to criminal convictions or suspected offences** (e.g., disclosures required for safeguarding, employment vetting, or regulatory compliance)

We ensure this information is handled with the highest levels of confidentiality and security, and only used when necessary for lawful, specific purposes—such as the provision of healthcare, employment, regulatory reporting, safeguarding, or public health.

WHO DO WE SHARE INFORMATION WITH?

To provide safe, effective, and coordinated care and services, the NERHA may need to share your personal and sensitive information with trusted third parties. This is done in compliance with data protection laws and under strict obligations of confidentiality and security.

SHARING WITHIN THE NERHA

Your personal and sensitive data may be shared within different departments of the NERHA to facilitate the processing of healthcare services, employment obligations, and other operational needs. This sharing is done on a need-to-know basis to ensure appropriate service delivery.

TYPES OF ORGANISATIONS WE MAY SHARE INFORMATION WITH

1. **Healthcare Providers**
   Your personal information may be shared with other healthcare providers involved in your care, such as hospitals, health centres, community health teams, specialist clinics, and care homes.
2. **Social and Community Care Services**
   We may share data with social and community care services, including agencies involved in providing welfare or support services relevant to your care.
3. **Third-Party Data Processors**
   Personal and sensitive personal data may be shared with third-party data processors such as IT service providers, software vendors, or analytics partners who support our systems and services. These third parties are contracted to maintain confidentiality and data protection standards.
4. **Public Health Authorities**
   We may share information with public health authorities such as the MOHW for health monitoring, disease prevention, and public health initiatives.
5. **Educational Institutions**
   Where required for training, clinical placements, or research under approved protocols, personal data may be shared with educational institutions and research bodies.
6. **Law Enforcement and Legal Authorities**
   Personal data may be shared with law enforcement or legal authorities when required for lawful investigation, crime prevention, or public safety.

WHEN WE ARE LEGALLY REQUIRED TO SHARE INFORMATION

In some cases, we are legally obligated to share personal information. Examples include:

- **Legal obligations**: Such as reporting notifiable diseases to public health authorities or responding to regulatory inquiries.
- **Court orders**: When required by a court for legal proceedings.
- **Public inquiries or investigations**: Where we are required to cooperate with public investigations.

SHARING INFORMATION IN THE PUBLIC INTEREST

We may also share your personal data without your explicit consent if there is a **compelling public interest** or when the need to protect individuals or the public outweighs the duty of confidentiality. This may include:

- **Preventing or detecting serious crimes**.

- **Managing serious risks** to the health and safety of the public, patients, or staff.
- **Protecting vulnerable individuals**, such as children or adults at risk of harm.

USE OF DE-IDENTIFIED (ANONYMISED OR PSEUDONYMISED) DATA

Where possible, we will remove or de-identify personal information before using it for secondary purposes beyond your direct care. This may include:

- **Legal and regulatory compliance**.
- **Health planning and service improvement**.
- **Research and public health monitoring**.
- **Safeguarding and risk management**.

All processing of de-identified data is done in accordance with applicable laws and regulations, with appropriate safeguards to protect your confidentiality.

INTERNATIONAL TRANSFERS

We take the privacy and security of your personal data seriously. If it is necessary to transfer your data internationally, we will only do so to countries that provide an adequate level of data protection or where we have put in place appropriate safeguards, such as standard contractual clauses or binding corporate rules.

Before any international data transfers take place, we will seek explicit consent from individuals unless an exception applies under the applicable privacy laws. Additionally, we assess the legal requirements and risks associated with such transfers to ensure the continued protection of your personal data.

WHAT IS OUR LAWFUL BASIS FOR USING INFORMATION?

Under the DPA, and where applicable, the GDPR, the lawful basis for processing your personal information depends on the specific circumstances and purposes of the processing. These are the legal grounds on which we rely to collect, use, and share your personal and sensitive data:

PERSONAL INFORMATION

1. **Consent**
   In certain situations, we process personal data based on **your explicit consent**. This means that you must provide your clear, informed, and unambiguous consent for specific uses of your personal information.
   Example: Consent is often required for certain activities such as marketing communications, participation in optional services (e.g., wellness programs), or the use of website cookies.
2. **Contractual Obligation**
   We may process your personal information to fulfil a contract with you or to take steps at your request before entering into a contract.
   Example: Employees' personal information may be processed for payroll, benefits, and other employment-related obligations. Service users may have their data processed as part of a contract for the provision of healthcare or services.
3. **Legal Obligation**
   In some instances, we are required by law to process personal data.
   Example: Legal obligations include the reporting of notifiable diseases to public health authorities, compliance with tax or employment laws, and fulfilling legal requests from courts or regulatory bodies.
4. **Public Interest and Public Health**
   Personal data may be processed where necessary for the **public interest** or for tasks carried out in the **public health sector**.
   Example: This includes data processed for disease prevention, health promotion, or responding to public health emergencies, such as pandemics or vaccination campaigns.

5. **Legitimate Interests**
   We may process personal data based on our legitimate interests or those of a third party, provided that these interests do not override your rights and freedoms.
   Example: Data may be processed to improve healthcare services, manage patient flow, or ensure efficient operation of healthcare facilities.

SENSITIVE (SPECIAL CATEGORY) DATA

Certain categories of personal data, such as **health data**, are considered more sensitive and require an additional lawful basis for processing. The following are the main lawful bases we rely on for processing sensitive personal information, such as health and care data:

1. **Health or Social Care**
   Personal health data may be processed when necessary for the provision of **health or social care services**.
   Example: We process health data to deliver healthcare, diagnose conditions, provide treatment, or manage your care needs.
2. **Public Health**
   Sensitive personal data related to public health, such as data for **disease prevention** or **public health monitoring**, may be processed under the lawful basis of public health.
   Example: Processing is necessary to manage public health crises, such as tracking and responding to infectious disease outbreaks.
3. **Employment**
   In certain employment-related circumstances, sensitive data may be processed for purposes such as payroll, or benefits.
   Example: Employees' health information may be processed for occupational health assessments or wellness programs.
4. **Legal Claims or Court Orders**
   Sensitive data may be processed when necessary for the establishment, exercise, or defence of legal claims, or when required by a court or tribunal.
   Example: This includes processing sensitive data in legal proceedings related to employment disputes or health-related claims.
5. **Substantial Public Interest**
   We may process sensitive data when necessary for a **substantial public interest**, in accordance with applicable laws.
   Example: Processing may be needed to protect public safety, safeguard vulnerable individuals, or support public health initiatives.
6. **Archiving, Research, and Statistics**
   We may also process sensitive data for **archiving, research, or statistical purposes** in accordance with applicable laws.
   Example: This could include the use of anonymised data for healthcare research or planning.

Note: In most cases, **consent** is not required for processing sensitive health data under the JDPA, as processing is often necessary for the provision of healthcare or the performance of official duties. However, we will always ensure that such data is handled with the utmost care, confidentiality, and in compliance with the law.

HOW LONG DO WE STORE YOUR DATA?

We retain your personal and sensitive personal information for as long as necessary to provide healthcare services, fulfil employment relationships, meet contractual obligations, and comply with legal and regulatory requirements.

RETENTION PERIODS

The retention periods for different types of data are determined based on:

- The type of record (e.g., medical records, employment records)

- The nature of the activity, product, or service provided
- Applicable local legal or regulatory requirements

In most cases, we will retain your personal data for no longer than required by law and per the **NERHA Data Retention and Data Disposal Policy**.

EXTENDED RETENTION

In certain situations, data may be retained for longer periods if we are unable to delete it due to legal, medical, regulatory, or technical reasons. Additionally, data may be kept to resolve disputes or enforce agreements, where permitted by applicable laws.

HOW WE STORE YOUR INFORMATION

Your personal information is securely stored in both physical and electronic formats, with safeguards to protect it from unauthorized access, loss, or damage. Where third parties are involved in storing or processing your data, we ensure that they comply with applicable data protection laws and contractual agreements.

HOW WE DISPOSE OF YOUR INFORMATION

When your information is no longer needed or has reached the end of its retention period, we take the following actions, depending on the nature of the data:

- **Secure Disposal**: We securely dispose of physical records (e.g., by shredding paper documents) and electronic records (e.g., by securely wiping hard drives, drilling) in accordance with legal standards for data destruction.
- **Archiving**: Some information, particularly historically significant records, may be archived.
- **Anonymisation or Pseudonymisation**: If your data is no longer required for direct care or legal obligations but may still be useful for research, public health monitoring, or other purposes, we may anonymize or pseudonymize the data to protect your identity.

WHAT ARE YOUR DATA PROTECTION RIGHTS?

We collect and process only the minimum data necessary to deliver safe, effective, and continuous healthcare and administrative services. We make every effort to ensure that the data we maintain is accurate, up to date, and protected from unauthorized access.

As a data subject under the DPA, you have specific legal rights concerning how your data is collected, used, and shared. These rights are outlined below:

YOUR RIGHT	WHAT IT MEANS
Right to Access	You have the right to request access to the personal data we hold about you, including whether and to what extent it is being processed.
Right to Rectification	If your data is inaccurate or incomplete, you may request that it be corrected or completed without undue delay.
Right to Erasure (Right to be Forgotten)	You may request the deletion of your personal data where it is no longer necessary for the purposes collected, unless required by law or for public interest (e.g. legal obligations or healthcare needs).
Right to Object to Processing	You have the right to object to the processing of your data, particularly where processing is based on legitimate interests or public interest.
Right to Restrict Processing	You can request that we temporarily restrict how we use your data, for example while a correction or objection request is being assessed.

YOUR RIGHT	WHAT IT MEANS
Right to Data Portability	Where processing is based on consent or a contract, and carried out by automated means, you can request your data in a structured, machine-readable format.
Right to Consent and Withdraw Consent	You have the right to give or withdraw consent to the processing of your data. If you withdraw your consent, it will not affect data already processed lawfully.
Right to Prevent Automated Decision-Making	You have the right not to be subject to decisions based solely on automated processing, including profiling, unless legally permitted or necessary for healthcare.
Right to Complain	You have the right to lodge a complaint with the **Information Commissioner**, the authority responsible for enforcing data protection in Jamaica.

HOW TO EXERCISE YOUR RIGHTS

If you wish to exercise any of your rights or express concerns about how your personal data is handled, you may contact the DPO of the NERHA using the contact details provided in the "Contact Information" section of this policy. We are committed to responding to all valid requests within the timeframes required by law.

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.

LINKS TO THIRD-PARTY WEBSITES

Our website may contain links to third-party websites for your convenience or reference. Please be aware that we are not responsible for the privacy practices, data handling, or content of these external sites. The NERHA strongly encourages all users to read and understand the privacy policies of any third-party websites before submitting personal data. Accessing these sites is at your own discretion, and by doing so, you agree to hold the NERHA harmless from any liability arising from the use of such websites.

HOW DO I COMPLAIN?

If you have any concerns about our use of your personal information, you can make a complaint to us at data.protectnerha@nerha.gov.jm.

Following this, if you are still unhappy with how we have used your data, you can then complain to the Office of the Information Commissioner (OIC).

The OIC's address is:
Masonic Building, 2nd Floor.
45 – 47 Barbados Avenue. Kingston 5
Email: info@oic.gov.jm
Phone: (876) 929-8568
Phone: (876) 929-6952
Phone: (876) 960-0874
Phone: (876) 968-5622

OIC website: https://oic.gov.jm/

CHANGES TO THIS PRIVACY NOTICE

NERHA reserves the right to make reasonable updates to this Privacy Notice as needed to accurately reflect how we collect and use your personal and sensitive information. We encourage you to review this Notice regularly to stay informed about our data practices and any changes that may occur.

DATE OF LAST REVIEW
July 7, 2025