NHI Bahamas
modern | affordable | accessible

National Health Insurance Authority

Privacy Policy

VERSION – April 20, 2017

NHI Bahamas
modern | affordable | accessible

Table of Contents

NHI Bahamas
modern | affordable | accessible

NHIA Privacy Policy

1. Purpose of document

National Health Insurance Bahamas ("NHI Bahamas") is the Government's programme for a modern, affordable and accessible National Health Insurance ("NHI") plan, beginning with primary health care.

Pursuant to the *National Health Insurance Act*, 2016 ("NHI Act"), the Government established the National Health Insurance Authority ("NHIA") to administer NHI Bahamas.

The NHIA is committed to the highest standards of privacy and information management. This document outlines the NHIA's operational policy for the protection of beneficiary personal health information that is collected, sent or received by the NHIA.

2. Definitions

Back-up data means data kept only for the purpose of replacing other data in the event of that data being altered, lost, destroyed or damaged.

Beneficiary means a person who is enrolled to receive benefits under NHI Bahamas.

Beneficiary Registry means the database of all individuals with an NIB number who may be beneficiaries under NHI Bahamas.

Benefits means the goods and services specified in the NHI Bahamas Primary Care Benefits Package, which can be found online at http://www.nhibahamas.gov.bs/whats-covered/

Data means information in a form in which it can be processed.

Data controller means a person who, either alone or with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Disclosure in relation to personal data means the disclosure of information extracted from such data but does not include a disclosure made directly or indirectly by a data controller to an employee or agent of theirs or to a data processor for the purpose of enabling the employee, agent or data processor to carry out their duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed.

Duty of care means that a person or organization is legally obligated to avoid acting in such a way that may cause harm in any form to others.

Enrolment means the business process for acceptance of an individual for health coverage under NHI Bahamas.

National Health Insurance Authority ("NHIA") means the Authority established under section 4 of the *National Health Insurance Act*, 2016.

NHI Bahamas means the National Health Insurance Plan, established by the *National Health Insurance Act*, 2016, that in collaboration with the Ministry of Health:

a) establishes the administrative framework and other necessary mechanisms to enable the provision of equitable, accessible, affordable and quality health care services to all eligible persons for the attainment of universal health coverage;
b) facilitates people-centred health care that meets the needs of the population;
c) provides plurality in the health care system with equal opportunity for public and private-sector participation;
d) promotes efficiency in health care administrative operations; and
e) enables sustainability through appropriate allocation of resources in health care.

NHI Act means the *National Health Insurance Act*, 2016.

National Insurance Board of The Bahamas ("NIB") means the organization charged with administering the National Insurance programme established by the *National Insurance Act*, 1972.

National Insurance number ("NI number") means the unique numerical code found on an individual's NIB Smart Card that identifies its named holder.

NIB Registration Data means personal information about individuals registered with the NIB – including the NI number – that is relevant for NHI Bahamas enrolment purposes.

NIB Smart Card means the electronically readable card issued by the NIB that provides validation that the individual to whom it is issued is registered with the NIB.

Personal data means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller.

Personal health information means identifying information about an individual in oral or recorded form, including information that:

a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
b) Relates to the providing of health care to the individual, including the identification of a person as a provider of health care services to the individual;
c) Relates to the individual's eligibility and/or ability to pay for different levels of health care coverage, including any past, present, or future payments for the provision of health care to the individual; or
d) Relates to any findings derived from the testing or examination of any body part or bodily substance of the individual.

Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —

a) organization, adaptation or alteration of the information or data;
b) retrieval, consultation or use of the information or data;

c) transmission of data;
d) dissemination or otherwise making available; or
e) alignment, combination, blocking, erasure or destruction of the information or data.

Primary health care means the outpatient, first level of health care that focuses on prevention, and addresses and coordinates essential health needs.

Provider means a licensed entity (corporate or unincorporated) approved by the NHIA to provide health care services for beneficiaries under NHI Bahamas.

Sensitive personal data means personal data relating to —

a) personal identification information, including address, gender, phone number, date of birth, email address, identifying social media names/handles and financial data;
b) racial origin;
c) country of origin;
d) political opinions or religious or other beliefs;
e) physical or mental health (other than any such data reasonably kept by an employer in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other purpose);
f) personal health information (defined above);
g) trade union involvement or activities;
h) sexual life; or
i) criminal convictions, the commission or alleged commission of any offence, or any proceedings for any offence committed, the disposal of such proceedings or the sentence of any court in such proceedings; and
j) Any other pieces of data that may serve to directly identify an individual

3. Overview of NHI Bahamas

NHI Bahamas provides access to quality health care services for Bahamian citizens or legal residents who meet statutory eligibility requirements, including the possession of an NIB Smart Card and the ability to demonstrate that they were legally resident in The Bahamas within the preceding six months.

NHI Bahamas will be implemented in stages, beginning with primary health care.

Eligible individuals are required to enrol in NHI Bahamas to access covered services as beneficiaries. Covered services are described in the NHI Bahamas Primary Care Benefits Package, which is available on the NHI Bahamas website at http://www.nhibahamas.gov.bs/whats-covered/

Covered services will be delivered by:

- primary care medical professionals (e.g., physicians, nurses);
- pharmacists;
- diagnostic imaging professionals; and
- laboratory professionals.

Participating primary care physicians associated with a registered primary care Provider facility will be responsible for coordinating the delivery of covered services to beneficiaries.

During enrolment, beneficiaries will select:

- a primary care Provider facility; and
- a primary care physician associated with that Provider facility.

Pre-existing medical conditions cannot disqualify an individual from enrolment in NHI Bahamas, and there is no waiting period to enrol for eligible individuals with pre-existing conditions. NHI Bahamas guarantees the ability to maintain eligible beneficiaries' National Health Insurance coverage regardless of diagnoses or amount of care required. There is no lifetime maximum benefit amount of coverage.

For non-covered services, individuals will continue to access care as they would today – for example, through existing public funding mechanisms, private health insurance, out-of-pocket payments or other means. Workplace-related injuries, industrial accidents and occupational diseases will continue to be covered by the NIB.

If an individual is covered by private health insurance, they are required to disclose this during enrolment for the purpose of coordinating insurance benefits. Information required includes the name of the insurer and the plan, as applicable and outlined in regulations.

4. Purpose of personal information in relation to NHI Bahamas

Personal information about enrolled beneficiaries – including personal health information, personal data and sensitive personal data – is collected and used by the NHIA for NHI Bahamas programme purposes.

Examples of personal information that the NHIA may require include an individual's name, gender, date of birth, email address, telephone number, residence address, dependents, signature, medical records, laboratory test results, insurance information and commentary or opinion about a person.

Data is only used for programme purposes. Programme purposes include, but are not limited to:

- delivery of health care services;
- beneficiary enrolment;
- Provider registration;
- payment processing and audit;
- fraud detection and prevention;
- monitoring and evaluation; and
- purposes relevant to public health or public safety.

Data may be shared with registered primary care physicians and Government agencies (e.g., NIB) as is required for the purposes listed above.

5. Requirements under the Data Protection Act

The Bahamas *Data Protection (Privacy of Personal Information) Act*, 2003, ("Data Protection Act") protects the privacy of individuals in relation to personal data and regulates the collection, processing, keeping, use and disclosure of personal information.

The *Data Protection Act* is not specific to personal health information. However in carrying out its duties, the NHIA acts in a number of capacities described by the *Data Protection Act* and its regulations. If there is any discrepancy between this operational policy document and the legislation or its regulations, the legislation takes precedence. If there is any discrepancy between the NHIA privacy policy and any other NHIA operational policy document, the privacy policy takes precedence.

5.1 Collection, processing, keeping, use and disclosure of personal data

The *Data Protection Act* requires an organization that collects data to comply with the following provisions:

- the data or the information must be collected lawfully and fairly;
- the data must be accurate and, where necessary, kept up to date (except in the case of back-up data);
- the data must —
  - be kept only for one or more specified and lawful purposes;
  - not be used or disclosed in any manner incompatible with that purpose or purposes;
  - be adequate, relevant and not excessive in relation to that purpose or purposes; and
  - not be kept for longer than is necessary, except in the case of personal data kept for historical, statistical or research purposes; and
- appropriate security measures must be taken to prevent unauthorized access to – or alteration, disclosure or destruction of – the data and against accidental loss or destruction.

5.2 Right of access

Per the provisions of the *Data Protection Act*, any individual who makes a written request to an organization that possesses his or her personal data has a right, within 40 days, to:

- be informed whether the data kept includes personal data relating to the individual;
- be supplied with a copy of the data; and
- where any of the information is expressed in terms that are not intelligible to the average person without explanation, the information must be accompanied by an explanation of those terms.

Thus, individuals have a right to a broad array of data and health information that may be in the possession of an organization, including:

- Medical records;
- Billing and payment records;
- Insurance information;
- Clinical laboratory test results;
- Medical images, such as x-rays;
- Wellness and disease management program files;
- Clinical case notes; or
- Any other information used to make medical decisions about the individual.

Organizations may use an individual's data to inform the development of an aggregated data set that is not personally identifiable and is no longer used to make decisions specifically about the individual. An individual does not have a right to access personal health information that is not used to make decisions about the individual or individuals like in an aggregated data set mentioned above. This may include:

- Quality assessments or improvement records;

- Patient safety activity records; or
- Business planning, development, or management records that are used for business decisions rather than to make decisions about individuals.

For example, an organization's peer review files or provider performance evaluations may be generated from and include an individual's personal health information, but might not be in the designated record set and thus, not accessible by the individual. However, the underlying personal health information from the individuals' medical or payment records used to generate the above types of excluded information is still accessible by the individual.

If any NHI Bahamas beneficiary would like to see or obtain a copy of their personal data or personal health information kept by the NHIA, please contact the NHIA Privacy Officer.

5.3 Right of correction or erasure

An individual is entitled to have corrected or, where appropriate, erased any data relating to him or her that was inappropriately collected. The organization possessing the data must comply with the request within 40 days.

5.4 Disclosure of personal data in certain cases

Per the *Data Protection Act*, any restrictions on the disclosure of personal data do not apply if the disclosure is:

- determined by the Minister with responsibility for Information Privacy and Data Protection or the Minister of National Security required for the purpose of safeguarding the security of The Bahamas;
- required for preventing, detecting or investigating offences or collecting any tax, duty or money owed to the Government, statutory corporation, public body or a local authority;
- required for protecting the international relations of The Bahamas;
- required urgently to prevent injury or damage to the health of a person or serious loss of property; or
- required by a rule of law or order of a court.

6. Beneficiary Knowledge and Consent

During beneficiary enrolment, eligible beneficiaries are informed of the NHIA's privacy policy and treatment of personal data. The NHIA obtains consent from the applicant to collect personal information and use it for NHI programme purposes only. Consent is required to complete enrolment.

Beneficiary contact information, such as an email address or cell phone number, is kept strictly confidential and used only to reply to or send information to a beneficiary, if authorized by the individual. Under no circumstances is e-mail or SMS text correspondence used by the NHIA to collect or communicate sensitive personal information.

7. Data governance

The NHIA, as the government agency responsible for administering NHI Bahamas, collects, processes, keeps, uses and discloses personal data in accordance with the *Data Protection Act* and *National Health Insurance Act*.

The Managing Director of the NHIA determines the purposes and manner in which personal data are processed.

The NHIA's Privacy Officer is designated by the Managing Director. The Privacy Officer is a member of the NHIA's senior management team with a strong understanding of the relevant laws that govern data protection in The Bahamas and may also possess a legal background, such as the Deputy Directory of Strategy, Legal and Policy.

7.1 Memorandum of Understanding between the NHIA and NIB specific obligations

A Memorandum of Understanding ("MOU") between the NHIA and NIB contains information regarding the sharing of data between each organization.

The NIB Smart Card is the primary means by which the NHIA determines eligibility to enrol in NHI Bahamas. For this purpose, the NHIA will receive and process personal data from the NIB for beneficiary enrolment. The NHIA also uses NIB registration data for other purposes directly relevant to administering NHI Bahamas (e.g., determining residency, rate setting, claims processing, fraud detection, audit).

The NHIA information technology ("IT") system is integrated with a relevant subset of NIB registration data for purposes directly relating to NHI Bahamas. The Director of the NIB remains the data controller for the data the NHIA receives from the NIB.

The NIB possesses the authoritative record of its registrants. Any changes to data that originate with the NIB are made in the NIB system and propagated to the NHIA. There is no feed of updates from the NHIA IT system to the NIB registrant data set (e.g., to record address changes, name changes, etc.).

The NHIA has access privileges and duty of care for a relevant subset of NIB data (e.g. NI numbers), which includes NHIA interactions with Providers.

Individual Providers are the data controllers for their facilities for claims and activity data that they hold for their beneficiaries. The NHIA has access privileges and duty of care for Provider data in order to carry out its responsibilities. The NHIA processes data, including for the purposes of adjudicating claims and detecting fraud.

7.2 Provider registration

The NHIA IT system is used by Providers to:

- verify that a beneficiary who receives covered benefits is enrolled in NHI Bahamas; and
- report Provider service activities.

During Provider registration, Provider facilities name a person or persons who will have online access to the NHIA IT system that enables processing of personal data.

For Provider facilities with multiple registered Providers (e.g., a primary care physician *and* a laboratory Provider), the users are authorized to act specifically on behalf of their respective unit. The same

individual may be named for multiple units, or different individuals may be designated for each unit at the discretion of the Provider facility.

Only persons from a Provider facility's pre-qualified list who are also authorized by the NHIA are permitted to access personal data. Under no circumstances can named persons give their user identification ("ID") and password to other individuals.

8. Training and Awareness

All NHIA staff:

- receive a copy of the NHIA Privacy Policy and the *Data Protection Act*;
- are made aware of their role-based privacy responsibilities; and
- receive annual training in privacy.

The NHIA requires all registered Provider staff who handle data related to NHI Bahamas and personal data related to enrolled beneficiaries to review the NHIA Privacy Policy and the *Data Protection Act.*

The NHIA also requires all registered Provider staff to complete privacy training before handling any data related to NHI Bahamas or personal data related to enrolled beneficiaries. This privacy training should be done on an annual basis. Each Provider facility must attest to the NHIA that their staff has completed training and provide a description of that training. These terms are included in the master agreement signed by each Provider facility with the NHIA.

Acceptable forms of privacy training include:

- a certified course in privacy (online or in-person) that is endorsed by the Office of Bahamas Data Protection Commissioner in conjunction with the NHIA; or
- a presentation made by the Office of Bahamas Data Protection Commissioner.

9. Security Safeguards

Privacy and information management are key components of the NHIA IT strategy.

Any information the NHIA collects from or about beneficiaries is transmitted through a secure server and is used only for the purpose for which it was collected. Only those with proper authorization and approval from the NHIA Privacy Officer are able to access or handle sensitive personal data, including personal health information. Efforts are in place to eliminate the opportunity for misrepresentation to gain access to the NHIA IT system and any privacy incidents will be acted upon swiftly. (See Section 10: Privacy incidents)

Any paper records containing sensitive personal data are located out of site or common areas so as to minimize incidental disclosure of information. When not in use, they are stored where there is controlled access through locked cabinets.

After their purpose has been served, all electronic and digital records located on an electronic storage device (e.g., CD-R, USB) must be physically destroyed or magnetically erased as per industry standards.

In addition, sensitive personal data must never be stored on a non-secure device (e.g., personal computer, mobile device).

Where a Provider has historically maintained personal data on a non-secure device prior to registering with the NHIA, the Provider must immediately modify their pattern of practices going forward to comply with the security safeguards outlined in the NHIA Privacy Policy.

Any hard copy documents containing personal health information that are to be disposed of must be discarded into designated paper shredding containers. They must not be discarded with regular garbage or recycling.

10. Privacy incidents

The NHIA will contain, investigate and address all privacy incidents or breaches.

All NHIA personnel are responsible for immediately reporting a privacy incident or breach to the NHIA Privacy Officer. It is the NHIA Privacy Officer's responsibility to report privacy incidents or breaches to NHIA management.

Any person reporting an incident, from the NHIA or otherwise, is required to provide a description of the incident or breach, the individuals involved and immediate steps taken, if any, to contain the incident or breach.

The NHIA extends whistleblower protection (i.e., confidentiality and immunity) to anyone who reports a privacy incident or breach.

All NHIA personnel are responsible for actively supporting the NHIA Privacy Officer in privacy incident or breach containment, investigation and remediation activities as needed.

The NHIA Privacy Officer works in conjunction, as appropriate, with the Office of Bahamas Data Protection Commissioner to address reported privacy incidents.

If you think the confidentiality of your personal health information has been compromised in any way or have questions about this policy, please contact the NHIA Privacy Officer.

11. Compliance Monitoring

The NHIA monitors compliance with this privacy policy on a routine basis. Compliance monitoring includes:

- confidentiality agreements;
- NHIA operational policies that outline privacy expectations;
- regular audits; and
- security controls.

The NHIA's Privacy Officer reports the results of compliance monitoring to the NHIA Board on a quarterly basis.