# Health Insurance Authority (HIA) Privacy Policy – Updated

*Effective date: 06 January 2026*

This Privacy Policy explains how the Health Insurance Authority (HIA) – Ireland's independent regulator of private health insurance, collects, uses, shares and protects personal data. It sets out how we comply with our obligations under the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Act 2018 (as amended), and the Health Insurance Act, 1994 (as amended).

This Notice applies to all personal data processed by the HIA in the course of carrying out our statutory functions, including interactions with members of the public, regulated undertakings, suppliers and other stakeholders.

**About the HIA's statutory role (Health Insurance Act, 1994)**

Under Section 21 of the Health Insurance Act, 1994 (as amended), the HIA's core functions include: managing and administering the Risk Equalisation Scheme; maintaining the Registers of Health Benefits Undertakings and Health Insurance Contracts; evaluating and analysing information returns; raising consumer awareness of rights and services; advising the Minister for Health; and monitoring the operation of the Act and developments in health insurance. The HIA is guided by the principal objective in Section 1A: to ensure access to health insurance without discrimination based on health risk status, age or sex, supporting intergenerational solidarity.

**1. Data Protection Officer (DPO)**

You can contact the HIA's DPO with any query about this notice or your rights:

Post:
Data Protection Officer,
Teach Beaux Lane,
Sráid Mercer Íochtarach,
Baile Átha Cliath 2,
D02 DH60

Beaux Lane House
Mercer Street Lower
Dublin 2
D02 DH60.

Ríomhphost/Email: dataprotection@hia.ie

Fón/Phone: +353 (01) 406 0080.

**2. Purposes of processing (why we use personal data)**

Personal data is processed only where it is necessary to carry out our statutory functions and responsibilities. These purposes include: -

• To handle consumer enquiries and complaints, including explaining rights and health insurance options, and providing information in relation to health insurance (s.21(d))

• To monitor and report on the operation of the Health Insurance Acts and the health insurance market (s.21, s.33)

• To manage and administer the Risk Equalisation Scheme, including processing claims from registered undertakings and operating the Risk Equalisation Fund (ss.11A–11G, s.11D)

• To maintain statutory registers: The Register of Health Benefits Undertakings (s.14) and The Register of Health Insurance Contracts (s.7AC)

• To evaluate and analyse information returns received from undertakings (s.7D–s.7E) and, where applicable, assess overcompensation (s.7F)

• To issue enforcement notices and exercise statutory investigative powers where necessary (Part IIIA ss.18A–18D; Part IIIB ss.18E–18G)

• To manage professional services contracts and suppliers (s.23) and administer levies (s.17), accounts and audits (s.32), and statutory reports (s.33)

**3. Lawful bases for processing (GDPR) – **how your rights apply****

We process personal data only where there is a lawful basis to do so, such as where

it is necessary for compliance with legal obligations and to perform official duties in the public interest. Depending on the context, other bases may also apply. We highlight the legal bases and your associated rights here:

**Legal obligation - Article 6(1)(c) GDPR :** Processing is necessary to comply with our legal duties under the Health Insurance Acts (e.g., maintaining statutory registers, operating the Risk Equalisation Fund, statutory reporting).

Your Rights: access, rectification, restriction (where applicable), and the right to complain to the DPC.

**Public task/official authority - Article 6(1)(e) GDPR :** Processing is necessary to perform our statutory regulatory functions under the Health Insurance Acts (e.g., monitoring, evaluation, enforcement).

Your Rights: access, rectification, objection (Art. 21), restriction, and the right to complain.

**Consent - Article 6(1)(a) GDPR:** Used only in limited circumstances (e.g., where you ask us to assist with a consumer query/complaint and provide information we wouldn't otherwise hold). You can withdraw consent at any time.

Your Rights: withdraw consent, access, rectification, erasure, restriction, portability (where applicable).

**Contract - Article 6(1)(b) GDPR:** Where we process data to enter into or perform a contract with vendors or consultants providing services to the HIA (s.23).

Your Rights: access, rectification, erasure, restriction, portability (where applicable), objection (where applicable).

**Vital interests - Article 6(1)(d) GDPR:** Rare; only where necessary to protect someone's vital interests.

Your Rights: access, rectification, restriction, and the right to complain.

**Special category data:** The HIA does not routinely process special category data in carrying out market monitoring and statistical functions. Information returns under section 7D expressly exclude personal data. In limited circumstances (e.g., when assisting with an individual consumer query or in employment contexts), we may rely on

- Substantial public interest - Article 9(2)(g) GDPR
- Explicit consent - Article 9(2)(a) GDPR
- Employment/social protection law – Article 9(2)(b) GDPR
- Legal claims – Article 9(2)(f) GDPR

Strict safeguards and data minimisation always apply.

**Your data protection rights**

Your rights under GDPR depend on the lawful basis for processing. These may include access, rectification, erasure, restriction, objection, portability and the right to complain.

**4. Categories of personal data we process[1]**

The types of personal data we process depends on your relationship with the HIA and the purpose of your interaction. We only collect the minimum data necessary for each purpose. Categories of personal data may include: -

• Identification and contact details you provide to us for enquiries/complaints (e.g., name, email, phone)

• Professional contact data of supplier or contractor personnel for contract management

• Limited identifiers provided by registered undertakings or public bodies as permitted by law (e.g., policy/contract identifiers where necessary and proportionate); the HIA seeks to avoid receipt of personal data for market monitoring where not required

• Website usage data and cookies (see Section 9 below for more information)

• Other categories of personal data as required by law or necessary for the HIA's statutory functions

[1] Note: Section 7D of the Health Insurance Act provides that certain information returns relate to aggregated market data and may not include personal data. Where personal data is provided inadvertently, we will take steps to minimise, secure, and, where appropriate, delete it.

## 5. Where we get your data

We obtain personal data from a variety of sources, always in accordance with data protection law and only where necessary for our statutory functions. These sources include: -

• Directly from you when you contact us by email, phone, phone recordings, online forms or other means

• Registered undertakings and other public bodies as permitted by law, for example information returns under s.7D of the Health Insurance Acts, or stamp duty information from Revenue as provided for by s.11C(4))

• Our processors/suppliers solely to the extent necessary to provide services to the HIA (s.23)

• Open sources where appropriate (e.g., published reports/statistics)

• Other sources as required by law or necessary for the HIA's statutory functions

## 6. Sharing your data (recipients)

We only share personal data where it is lawful, necessary and proportionate to do so, always in line with our statutory functions. Recipients of personal data may include: -

• The Minister for Health and the Department of Health, to fulfil statutory reporting and advisory functions (s.33);

• The Comptroller & Auditor General in respect of audits of the Risk Equalisation Fund (s.11D(9)–(10)) and other statutory audits;

• Courts and tribunals, where required by law, including enforcement of statutory powers (Part IIIA & IIIB) or in connection with legal claims;

• Service providers and consultants acting under contract and subject to GDPR (s.23) and contractual safeguards;

• Other recipients as required by law or necessary for the HIA's statutory functions.

We disclose contents of information returns only where necessary for our statutory functions (s.7G). We do not sell personal data or share it for marketing purposes.

## 7. International transfers

We do not routinely transfer personal data outside the European Economic Area (EEA). If it becomes necessary to transfer personal data internationally, (for example, where an IT or cloud service provider involves support or processing from outside the EEA), we will ensure that appropriate safeguards are in place as required by law. These safeguards may include: -

• An adequacy decision by the European Commission (confirming that the destination country provides an adequate level of data protection

• Standard Contractual Clauses approved by the European Commission

• Other appropriate safeguards as required by data protection law

## 8. Retention (how long we keep data)

We retain personal data only for as long as necessary to fulfil the purposes set out in this Notice and to meet our legal, accounting, or reporting requirements, and the HIA's records management policies. Statutory records relating to the Risk Equalisation Fund, registers, audits and reports may have specific retention obligations under the Health Insurance Acts (e.g., ss.11D, 32–33).

## 9. Cookies and website analytics

Our website uses cookies to provide a secure, reliable and user-friendly experience. Cookies are small text files stored on your device to help us remember your preferences and understand how visitors use our website.

We use necessary cookies to enable core website functions and analytics cookies to general technical data (e.g., IP address, browser type) for statistical purposes, helping us improve our services. We do not use cookies to identify you unless you choose to provide information (for example by submitting a form). You can control or disable cookies through your browser settings.

## 10. Your data protection rights (GDPR Articles 12–22)

Under data protection law, you have a range of rights regarding your personal data. These rights depend on the lawful basis for processing and the specific circumstances. Your rights include: -

• The right to be informed about how your data is used (Art. 12-14)

• Right of access to your personal data (Art. 15)

• Right to rectification of inaccurate or incomplete data (Art. 16)

• Right to erasure ("right to be forgotten") in certain circumstances (Art. 17) – subject to legal obligations

• Right to restriction of processing in certain circumstances (Art. 18)

• Notification of rectification/erasure/restriction (Art. 19)

• Right to data portability (Art. 20) – where processing is based on consent or contract and carried out by automated means

• Right to object to processing in certain circumstances (Art. 21) – particularly where processing is based on public task/official authority

• Rights related to automated decision-making, including profiling (Art. 22)

To exercise your rights, contact dataprotection@hia.ie. We may need to verify your identity. You also have the right to lodge a complaint with the Data Protection Commission (www.dataprotection.ie; 21 Fitzwilliam Square South, Dublin 2; info@dataprotection.ie; +353 1 765 0100 / 1800 437 737).

**11. Recruitment Data Processing**

Personal data provided as part of a job application (including CVs, cover letters, interview notes, and references) is processed for the purpose of assessing suitability for employment, conducting interviews, making hiring decisions and fulfilling our legal and regulatory obligations.

The legal bases for processing are: -

• Taking steps prior to entering into a contract - Article 6(1)(b) GDPR

• Compliance with legal obligations - Article 6(1)(c) GDPR

• Our legitimate interests in managing recruitment - Article 6(1)(f) GDPR

Special category data (such as health or disability information) is processed only where necessary and in accordance with Article 9 GDPR.

Recruitment data is retained for up to **18 months** after completion of the recruitment process, unless a longer period is required by law (for example, a legal hold). After this period, your personal data will be securely deleted.

Data subjects have all rights under GDPR, including access, rectification, and erasure.

**12. Security**

We take the security of your personal data seriously. We apply appropriate technical and organisational measures to protect personal data against unauthorised access, loss, alteration or disclosure. These measures may include access controls, encryption, contractual safeguards with processors, and staff training. Access to personal data is restricted to personnel who need it for their statutory or contractual duties.

**13. Changes to this Privacy Policy**

We may update this Privacy Policy, from time to time, to reflect legal or operational changes, or best practice. The effective date of the current version appears at the top of this document.

**Annex – Key statutory references**

The following laws and regulations underpin the HIA's data protection obligations and practices: -

• Health Insurance Act, 1994 (as amended): Sections 1A (principal objective), 7AB–7AC (contracts/register of contracts), 7C (certain information incl. PPSN), 7D–7E (information returns; evaluation/analysis), 7F (overcompensation), 7G (disclosure of information returns), 11A–11G (Risk Equalisation Scheme), 11D (Risk Equalisation Fund), 14–18 (registration; levy; records), Part IIIA (ss.18A–18D) enforcement notices, Part IIIB (ss.18E–18G) authorised officers and powers, 21 (functions of Authority), 32–33 (accounts, audits, reports), 34 (disclosure of information).

• GDPR: Articles 5 (principles), 6(1)(a)–(f) (legal bases), 9(2) (special category conditions – notably (a) consent and (g) substantial public interest), 12–22 (data subject rights), Chapter V (international transfers).

• Data Protection Act 2018; National Archives Act 1986.

| Version | Date | Author | Changes Made | Approved by |
|---|---|---|---|---|
| 1.0 | 10/2024 | Cora Rattigan (DPO) | Not Original | SMT |
| 2.0 | 12/2025 | Sandra Eaton | * Updated statutory references throughout, explicitly cited the Health Insurance Act, 1994 (as amended), GDPR, Data Protection Act 2018 (as amended), and National Archives Act 1986.<br>* Expanded and clarified the "Purposes of Processing" section to map directly to HIA's statutory functions under Section 21 and Section 1A of the Health Insurance Act.<br>* Added a detailed section on lawful bases for processing, highlighting GDPR Articles 6(1)(a)–(f), Article 9(2) (special category data), and the rights associated with each basis.<br>* Enhanced the "Data Subject Rights" section to explicitly list all rights under GDPR Articles 12–22, with clear instructions for exercising these rights.<br>* Clarified the categories of personal data processed, including website usage data and cookies, and referenced the relevant policy section.<br>* Improved the "Sharing of Data" section to specify statutory grounds for sharing, including references to relevant sections of the Health Insurance Act (e.g., s.11C(4), s.33, s.7G).<br>* Added a section on international data transfers, referencing GDPR Chapter V.<br>* Updated the retention policy to reference the National Archives | SMT |

| | | | | |
|---|---|---|---|---|
| | | | Act 1986 and statutory retention obligations.<br>* Included an annex listing all key statutory references cited in the policy.<br>* Incorporated best-practice language and structure from the Department of Social Protection's Privacy Statement, where relevant and within the scope of HIA functions.<br>* Minor formatting and language updates for clarity, transparency, and compliance. | |