

Data Protection Notice to Members/Associate Members *(Effective from March 2018, updated March 2026)*

Members/associate members are encouraged to read this notice which sets out essential information about the personal data we collect from you, how we use and safeguard this information, who we share it with and why, and how long we will keep it on file. It also explains your rights, arising from the General Data Protection Regulation (GDPR).

Please also bring this notice to the attention of anyone who is covered by your policy with St. Paul's Garda Medical Aid Society (the Society).

1. Who we are

St. Paul's Garda Medical Aid Society has been looking after the health insurance needs of its members since the 1st of January 1980 when it formed from the amalgamation of the Garda Síochána Medical Aid Society and the St. Paul's Benefit Society Limited.

The Society operates as a private Health Insurance Scheme and is a "Restricted Membership Undertaking". This means that membership of the Society is confined to members of the Garda Síochána, Student Gardai, Retired members of An Garda Síochána, Widow, Widower and Partner of deceased members of An Garda Síochána and former members entitled to a deferred Garda Pension, all of whom are, or were, holders of the Society's Comprehensive Health Insurance Contract at retirement or leaving the Force, all of whom are paying the current subscription to the Society. It also includes staff of the Society as members. It also includes those who are entitled to seek associate membership through their connection with a member as the adult child of a member who can add on their own spouse/partner and their children as associate members. They will be policyholders.

Members of the Society, except those excluded under the Society's Rule 2, may nominate "dependents" who may include the Spouse or Partner of the member, children of the member including adopted or fostered children and partners children when the partner is a nominated dependent and on cover with the Society. Spouses, Partners and children of the member of the Society are therefore nominated "Dependents."

An associate member means a non-voting member of the Society, that shall not attend or vote at any general meetings of the Society. Associate members include dependants as defined in Rule 66(k). Voting members' children reaching adulthood may continue as associate members and may include their spouses, partner and children as associate members.

The Society is registered with the Health Insurance Authority and is operated in accordance with Irish Health Insurance Legislation. Its licence is granted by the Health Insurance Authority and is renewable on a year-to-year basis.

2. Our approach to Data Protection

We have always appreciated your trust in us to collect, process and protect your personal information and we will continue to look after your information in a way that merits your

trust. We are committed to meeting our obligations under the GDPR and have appointed a Data Protection Officer (DPO), who has oversight of our information practices and is responsible for ensuring your rights are fulfilled. The DPO is also a point of contact for members/associate members should you have any questions or concerns about your personal information.

In the context of the GDPR and the Data Protection Acts (1988 as amended), St. Paul's Garda Medical Aid Society is the data controller¹

You can contact our DPO at dpo@medicalaid.ie or write to: Data Protection Officer, St. Paul's Garda Medical Aid Society, Suite 4, Plaza 255, Blanchardstown Corporate Park 2, Ballycoolin Rd., Dublin 15, D15 NA7D²

3. The information we collect and hold about you and others covered by your policy

Most of the information we collect from you is personal, and some of it is very private to you, including information about your health and that of your family. This type of information is treated as a "special category", meaning that we apply stringent safeguards against its improper use or disclosure.

We collect and store only the information that we need to look after your health insurance business, and this will include:

Information about you as the member/policyholder

- **Your personal identification and descriptors**

- Full name/Maiden name/Signature
- Home address; email address; phone number and other contact information
- Age/date of birth
- Gender
- Marital status
- Partner/spouse and dependents
- Pension number, Pay number and place of work
- Tax Identification Number/PPS Number
- Proof of identity and address e.g. copy of driving licence/passport and utility bills
- IP address
- Biometric data including photographic ID, dental chart and voice (call) recordings

¹ GDPR, Article 13 (1)(a)

² GDPR, Article 13 (1)(b)

- **Your health and related information**
 - Health Records
 - Medical histories
 - Information about injuries and accidents
 - Records of treatments obtained by you
 - Length of any stay in a hospital
 - Other treatments or services received by you
 - Previous insurance history
 - Personal bank account or credit union account details
 - Payroll, credit or payment card details
 - Other information relevant to a claim

Information about other persons currently or previously covered by your membership/policy

- **Personal identification and descriptors, including the relationship to you as the policyholder, including:**
 - Full name and PPSN number of your spouse, partner and children.
 - Verification of the age of a minor child or adult e.g. by provision of a birth certificate
- **Health and related Information**
 - As above.

4. How we collect this information

We record and file the identification and contact information and other data that you input into our online or printed forms or provide to us over the phone when you join the Society.

We can only deal with and communicate with the member/policyholder, so when you contact us we may need to verify your identity, for example by asking you a security question or looking for some additional personal detail that only you would know.

When we need information about a family member or any other person(s) covered by your policy, we will obtain that information from you, as the member/policyholder.

We will record and/or make notes about phone conversations.

Our website makes limited use of 'cookie' technology. A cookie is a piece of text that our server places on your device when you visit our website. The type of cookie we use is "a non-persistent session enabler" which means it is used only to allow your device to

communicate with the site while you log-in and use the site; the cookie expires when you log out of the site. We also collect the IP address of any device which is trying to connect with the site and use this to track successful or failed attempts at log-in to your account and the number of attempts made.

5. Information from other sources³

We may seek relevant information about your health, medical conditions and any treatments or other services received by you or other person(s) covered by your policy: this information will generally come from you, but we may also request and obtain it from your physician, a hospital or other treatment centre, or your family members. This type of information is needed to administer claims and is not used for any other purpose.

We may also seek information, where we have a personal undertaking with our Member/associate member relating to any third-party claim, from relevant parties, for example: An Garda Síochána, the Personal Injuries Bord, Legal representatives or other such persons.

6. How we use your information⁴

We use information about you and others covered by your policy to:

- Set up, amend or renew your policy.
- Manage your health insurance policy.
- Set your subscription rate.
- Provide health insurance services to you as a member/associate member.
- Process your health insurance claims and associated payments.
- Check and verify aspects of claims including treatments, duration of stays and convalescence options applied or utilised by medical service providers.
- Respond to your requests and provide information.
- Respond to statutory obligations or requests from the courts and enforcement authorities.
- Audit Medical Service Providers.
- Keep our records up to date to contact you when required and provide the best customer service.
- Produce internal management information to run our business and identify ways in which we can improve our services.
- Provide relevant information to other health insurance providers in the event of you switching provider; and.

³ GDPR, Article 14 (1)(c)

⁴ GDPR, Article 13 (1)(c)

- Perform any other health insurance related activities which we are obliged to undertake, or which we have gained your consent to perform

7. Our lawful basis for processing⁵

To process your information lawfully, we rely on one or more of the following legal bases:

- Provision of a policy of health insurance (the performance of a contract);
- Legal obligation.
- Our legitimate business interests.
- Your consent; and,
- Protecting the vital interests of you or others

Some examples for each lawful basis are given below. Please note that some information is processed under more than one lawful basis:

Lawful basis	Examples of what we use your information for
<p>Performance of a contract – between you and us, or in order to take steps prior to entering into a contract between you and us</p> <p>Provision of a policy of health insurance or health-related insurance - processing your information is necessary for us to provide you with services. If you do not provide the information we need, or help us keep it up to date, we may not be able to provide you with services and may have to terminate your membership.</p>	<p>We process your information to identify and authenticate you to use our services.</p> <p>When you ask to join the Society, we must assess your eligibility to do so. When you sign the application form, this is a contract in which you are agreeing to comply with the rules of the Society.</p> <p>Similarly, when you submit a claim to us we must assess your claim in line with our policy with you.</p> <p>As part of our membership agreement with you, we have the right to collect payment or money owed to us, to include refunds for claims made which were subject to a third-party case of compensation.</p>
<p>Legal obligation – we must process this information to comply with our legal obligations.</p>	<p>We process your personal information to identify and authenticate our members/associate members.</p> <p>We share your information with third parties when obliged to do so.</p>

⁵ GDPR, Article 14 (1)(c)

	<p>We must continually monitor and update information to ensure your data is safe, accurate and up to date. This ensures we keep your personal details secure and give you the best customer service.</p> <p>We continually monitor electronic devices to detect and prevent fraud and cyberattacks. This enables us to protect and secure our member/associate member and business information, our IT system and networks and our business interests.</p>
<p>Our legitimate interests – means the interests of the Society in conducting and managing our business when providing health insurance services. Core legitimate interests of the Society are to provide the best customer service, to protect our members/associate members and employees, and to grow our member/associate member base to remain vital and viable⁶.</p> <p>We will assess whether the legitimate interest of the Society will affect your rights and freedoms as a data subject prior to processing. We implement safeguards to ensure that the processing remains fair and balanced.</p> <p>You have the right to object to being included in processing where the lawful basis used is legitimate interest.</p>	<p>We produce internal management information and models to ensure necessary safeguards are in place and to assess the effectiveness of these.</p> <p>We send out marketing materials to our members/associate members to promote ourselves, our products and services.</p>
<p>Your consent – we require your consent for processing certain information and will ensure this is obtained under the principles:</p>	<p>With your consent, we will let you know about new services you might like to avail of. We may do this by post, email, or through digital media.</p> <p>We encourage email communication where possible and we will primarily contact you via e-mail unless you request</p>

⁶ GDPR, Article 13 (1)(d)

<ul style="list-style-type: none"> • Free will – your consent must be freely given and not influenced by external factors • Specific – we will be clear on what exactly we are asking your consent for • Positive action - clear affirmative action is required. We will not use pre-ticked boxes, or imply or assume your consent • Recorded – we will keep a record of your consent and how and when obtained • Right to withdraw – we will stop any processing that requires your consent once you request this; you can withdraw your consent at any time. 	<p>it via paper or hard copy contact through the ordinary mail.</p> <p>If we ever contact you to get your feedback on ways to improve our services, you have the choice to opt out.</p>
<p>Protecting the vital interests of you or others</p>	<p>Sharing information to serve you</p> <p>Should a situation arise where you are incapacitated and unable to communicate for yourself, we may share health insurance related information with your next-of-kin, immediate family, authorised representative⁷ or medical professionals. This is to ensure you receive your full insurance cover and benefits and to protect your best interests and those of your family.</p>

8. How we keep your information safe.

The safety of your information and data is very important to us. We keep our computers, files and buildings secure. Hard copy files are kept in organised and secure storage areas. Claims are filed by Claim Number, not by members registered number. We are moving to virtual storage of files virtual cloud (including iCloud) with encryption and backup measures to ensure accessibility and protection against loss or unauthorised access.

Transit of paper files is strictly limited. Where necessary to have member/associate member information available for e.g. Management Committee meetings, the

⁷ In line with The Assisted Decision-Making (Capacity) Act 2015, as amended

Management Committee members sign a confidentiality document on taking up their position as a member of the Management Committee. Meeting rooms are secure, and no member/associate member information is left in the open or on view to external parties.

Incoming post is brought directly to our office and opened by our staff. Outgoing mail from our office is posted through An Post.

We follow the standard of encryption in transit and at rest. Electronic copy files are stored on our proprietary IT system which requires user authentication to access it. Back-ups of electronic files are stored securely by our IT Service provider. Laptops are encrypted at hard-drive level. Use of memory sticks and other portable drives is limited, restricted to management personnel, and all external drives are encrypted. Data will be securely stored in the virtual cloud (including iCloud) with encryption and backup measures to ensure accessibility and protection against loss or unauthorised access.

All files and hard drives being disposed of are shredded and this is certified by the contracted Shredding Company.

When you contact us by phone to ask about your information, we will ask you to verify your identity.

9. How long we keep your personal information for.

To meet our legal and regulatory obligations, we hold your information while you are a member/policyholder and for a period of time after that. We do not hold it for longer than necessary. To help you understand how long we hold your data for, we have summarised our internal retention schedules below.

Please note that these retention periods are subject to legal, regulatory and business requirements, which may require us to hold the information for a longer period. For example, we must meet minimum retention standards for our Health Insurance requirements and also for Legal Refund cases; a prior claim may have a bearing on a current claim; legal cases can go on for protracted periods.

To meet such needs and to protect your interests as well as the Society's interests, we may need to hold data for longer than our internal schedules dictate. However, we will not retain data that is no longer needed, and we continuously assess and delete data to ensure it is not held for longer than necessary.

Document Type	Example Document	Retention Period
Details of Health Insurance Coverage with Society	Membership/policyholder details including details of persons who were Insured by the Society on Members/Associate Members Policy.	At least 20 years from cover ending with Society as per existing legislation (S.I. 312/2014).

Account and service information	Membership/policyholder account opening documents <ul style="list-style-type: none"> Letter of confirmation from previous insurer confirming level of cover Pay/employee number. Place of work – updated by member/associate member as necessary Bank/Credit Union details; IBAN PPSN 	At least 6 years beyond account closure or the member/policyholder’s death
	Account operation records including: <ul style="list-style-type: none"> member/policyholder instructions, communications and complaints Receipts Records of treatments received or refused under the policy Refunds and payments 	At least 6 years beyond account closure or the member/policyholder’s death
Other records	<ul style="list-style-type: none"> Records relating to legal claims 	At least 6 years beyond closure of the case
Revenue/Tax documentation	<ul style="list-style-type: none"> Tax Relief at Source information 	At least 6 years beyond account closure or the member/policyholder’s death

10. Your information and third parties

Sometimes we share your information with third parties. We expect these third parties to have the same levels of information protection that we have, and we expect that they provide sufficient guarantees that the necessary safeguards and controls have been implemented to ensure there is no impact on your data rights and freedoms.

We share your personal information and personal information of other person(s) covered on your policy with hospitals and medical professionals/consultants/care providers when necessary to aid the efficient processing of claims.

We share it with persons or companies with whom we do business with and who provide products or services e.g. IT Services that we use in conducting our business, including managing our relationship with our members/associate members. Similarly, we may share or disclose personal data to professional advisers, e.g. Legal advisers, accountants, whom

we may engage for any reasonable purpose in connection with our business, including assistance in protecting our rights. We will only share or disclose to these parties the information that they need to provide the products or services and will expect those parties to ensure that the information is always adequately protected.

We also must share information with third parties to meet any applicable law, regulation or lawful request including dealing with complaints. For example, we have a legal obligation under the Health (Provision of Information) Act 1997 to provide information to the National Cancer Registry Board, the Minister for Health or the HSE, hospital or other body or agency participating in any cancer screening. In all such cases, we will only disclose the minimum amount of information required to satisfy our legal obligation.

In the event you switch to another insurer, we will share your information with the new insurer in accordance with the Health Insurance Act 1994 (Determination of Relevant Increase under section 7A and Provision of Information under section 7B) Regulations 2014 and its subsequent amendments to confirm information that you have provided on taking out a policy with the new insurer; and Statutory Instrument No. 79/2015 - Health Insurance Act 1994 (Open Enrolment) Regulations 2015 and its subsequent amendments to facilitate the determination of maximum waiting periods and to confirm details of how long you and your dependents have been insured with us.

We share members' names and addresses with declared candidates seeking to be elected to the Management Committee of the Society.

11. International transfers of data

We may transfer your personal information outside of the Republic of Ireland where necessary to administer or manage your health insurance or related claims.

12. Your personal information rights

This section sets out your rights, when they apply and our responsibility to you. The exercise of your rights might be subject to certain conditions, and we might require further information from you before we can respond to your request. You may exercise your rights by contacting our Data Protection Officer at: dpo@medicalaid.ie or write to: Data Protection Officer, St. Paul's Garda Medical Aid Society, Suite 4, Plaza 255, Blanchardstown Corporate Park 2, Ballycoolin Rd., Dublin 15, D15 NA7D

Accessing your personal information (Right of Access)

As a member/policyholder, you can ask us for a copy of the personal information we hold and further details about how we collect, share and use your personal information. You can request the following information:

- the purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations,

- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
- where the personal data are not collected from the data subject, any available information as to their source,
- the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Updating and correcting your personal details (Right to Rectification)

You can easily edit or update your personal and contact information through the “Members/Associate Members” section of our website or by contacting us by email or letter. You will need your member/associate member number / registration number and a password to access the site.

If you contact us over the phone to edit or delete any information on your behalf, we will ask you questions to verify your identity.

Removing consent

Where we process your data solely based on your consent, i.e. for direct marketing purposes or to obtain feedback from you about our services, you are entitled to withdraw your consent to such processing at any time. You can do this by contacting us by email or letter.

Ask us to suspend processing your personal data (Right to Restriction)

You may have the right to restrict or object to us processing your personal information. We will require your consent to further process this information once restricted. You can request restriction of processing where:

- You believe the personal data is inaccurate, and you request restriction while we verify the accuracy.
- You believe the processing of your personal data is unlawful, and you request restriction of processing while we verify the accuracy.
- You require the data for the establishment, exercise or defence of legal claims but we no longer require the data for processing.
- You disagree with the legitimate interest legal basis and processing is restricted until the legitimate basis is verified.

Deleting your information (Right to be Forgotten)

You may ask us to delete your personal information, or we may delete your personal information under the following conditions:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- you withdraw your consent where there is no other legal ground for the processing.
- you withdraw your consent for direct marketing purposes.
- you withdraw your consent for processing a child’s data.
- you object to automated decision making.
- the personal data have been unlawfully processed.
- the personal data have to be erased for compliance with a legal obligation.

A request to delete your personal information cannot place this Society in conflict with existing legislation requiring the retention of the information.

Moving your information (Right to Portability)

Where possible we can share a digital copy of your information directly with you or another organisation.

We will provide this information in a structured, commonly used and machine-readable format. Note, we can only share this information where it has been processed electronically (hard copy documents are excluded for portability) and was processed either under your consent or under the lawful basis of provision of a policy of health insurance or health-related insurance. In line with GDPR guidance, information that is processed to satisfy a legal obligation or that we process as part of our legitimate business interests, will not be regarded as portable (see section 6 “how we use your information”).

Ask us to stop processing your personal data (Right to object)

Where we are sending you direct marketing materials and newsletters, or we are using your personal data for profiling purposes for direct marketing, you can ask us to stop doing so.

Automated Decision-making

We do not use automated decision-making in providing our services to you.

Restrictions and Charges

You should note that the exercise of your rights might be subject to certain conditions or restrictions. Where this happens, we will let you know.

Additionally, your our right to obtain information cannot adversely affect the rights and freedoms of others. Therefore, we cannot provide information on other people unless legally obliged to do so.

Usually, there is no charge when you contact us to ask about, or seek copies of, your information. If requests are deemed excessive or manifestly unfounded or unreasonable, we may charge a reasonable fee to cover the additional administrative costs, or we may choose to refuse the requests.

13. Making a complaint

If you have a complaint about how we are using your personal information, please let us know, so that we can endeavour to put things right as quickly as possible. If you wish to make a complaint you may do so in person, by phone, by letter or by email. Please be assured that all complaints received will be fully investigated. You can register a complaint through our DPO, and we ask that you provide as much information as possible to help us resolve your complaint quickly.

You can also complain directly to the Data Protection Commission, and their contact information is:

- Email: info@dataprotection.ie
- Phone: +353 (0) 1 765 0100 or 1800 437 737
- Write to: Data Protection Commission, 6 Pembroke Row, Dublin 2, D02 X963

14. Updates to this notice

We will make changes to this notice from time to time, particularly when we change how we use your information, such as in response to changing legal, technical or business developments. When we update it, we will take appropriate measures to inform you, consistent with the significance of the changes we make. You will always find an up-to date version of this notice on our website at www.medicalaid.ie or you can ask us for a copy.