General Data Protection Regulation (GDPR) Statement

The Plan's Processing of Personal Data Under the European Union (EU) GDPR, and Your Rights

The Plan makes all reasonable efforts to abide by the GDPR when required. That includes our affiliates and subsidiaries, as applicable. Personal data received from the EU and processed by The Plan is safeguarded in a manner similar to how protected health information is safeguarded under the Health Insurance Portability and Accountability Act (HIPAA).

The GDPR requires that personal data from the EU/European Economic Area (EEA) be treated with special protection. It also provides EU/EEA-based individuals (defined as "Data Subjects" under the GDPR) with certain individual rights with respect to their personal data. These Data Subject rights include:

1. The right to be informed about the collection and use of their personal data.
2. The right to access their personal data.
3. The right to correct their personal data if it is inaccurate or incomplete.
4. The right to erasure/deletion by requesting removal of certain personal data where there is no compelling reason for its continued processing.
5. The right to restrict (to 'block' or suppress) processing of personal data.
6. The right to obtain and possess their personal data (portability) for their own reuse.
7. The right to object to the processing of personal data under certain circumstances.
8. Rights in relation to certain kinds of automated decision-making (making a decision solely by automated means without any human involvement), and profiling (automated processing of personal data to evaluate certain things about an individual).

We will make reasonable attempts to accommodate requests by Data Subjects to exercise the rights listed above. Where necessary, we have implemented compliance measures, including internal data protection policies and maintaining documentation on our processing activities. We have also appointed a Data Protection Officer in accordance with GDPR requirements.

In order to inform Data Subjects and enable the exercise of rights under the GDPR, we are making the following disclosures about personal data processing subject to the GDPR (this "GDPR Statement"). For purposes of this GDPR Statement, references to "we," "us," or "our" mean the Plan and its affiliates as applicable, and references to "you" and "your" mean the Data Subject.

I. How we use personal data

We use personal data for three general purposes: to provide medical care and advice, for insurance and health benefits administration, and for related administrative and corporate affairs (collectively, the "Services").

The medical care purposes include but are not limited to: providing evaluation and treatment, consulting or coordinating with other providers of care, conducting quality assessment and improvement activities, and maintaining your medical records.

Insurance and health benefits administration purposes include but are not limited to: enrolling members for coverage, processing claims and sending explanations of benefits, responding to coverage-related questions, providing care management and wellness programs, reporting financial and other data to our clients, and conducting fraud prevention.

Our administrative and corporate affairs purposes include but are not limited to: accepting and processing applications for employment or similar workforce affiliation (e.g., internships), maintaining personnel and employment-related records, conducting client billing activities, and developing and marketing new products and services.

II. Who receives personal data?

Members of our workforce receive personal data in connection with our provision of the Services to you. In addition, we share personal data as necessary with certain third parties who contract with us to assist in the delivery of Services. We also share personal data with clients (e.g., group health plan customers) and some of their vendors as necessary and appropriate to conduct business activities.

III. How long is personal data stored?

Generally, we store personal data for as long as is necessary to provide the Services, and for a reasonable retention period in accordance with applicable law and industry standards. Our usual storage period is seven (7) years, unless dictated otherwise by legal requirements and/or our corporate policies.

IV. Your rights with respect to your personal data

You have the right at any time to exercise your Data Subject rights, including the right to: request access to and correction or erasure/deletion of personal data that we hold, request restriction of processing of your personal data, and obtain and possess data about you (portability). Your full list of rights is reflected above. If you would like to exercise any of these rights, please send a written request to our Data Protection Officer at the address listed below.

Not all requests can be granted. If your request is denied, you will be provided with the reason for the denial.

V. Withdrawal of consent to process personal data

We collect consent for processing personal data of EU/EEA-based individuals. You have the right to withdraw consent at any time. You must withdraw your consent in writing, addressed to the Data Protection Officer listed below. In order to ensure timely and accurate fulfillment of your withdrawal, you must include your name, address, your Member Identification Number (if the withdrawal is directed to the Plan concerning your health insurance coverage), and the specific processing activity(ies) for which you no longer consent. Withdrawing consent will not affect the lawful processing activity(ies) that took place previously based upon the consent you provided before the withdrawal.

VI. Complaints

You have the right to file a complaint with the appropriate data protection authority in the EU/EEA.

VII. Sources of personal data and legal basis for our personal data processing

We may receive personal data from you, from your providers of medical care, from your employer, and from other third parties in connection with the provision of Services. We need to process your personal data, such as name, address, and medical and insurance information, regardless of who provides it, in order to provide the Services described above and to carry out lawful business operations.

VIII. Is personal data used for automated decision-making or profiling?

We may use automated decision-making processes and profiling in the performance of our insurance and health plan administration contracts. For example, claims processing is primarily an automated process. We use profiling to help identify individuals who could benefit from care and case management, medical and prescription management, and other programs or wellness initiatives offered as part of the health benefits contract. We also use profiling to identify opportunities for communication with you about various programs, offerings, or important notices.

IX. Location of personal data processing

All personal data processing occurs in the United States.

X. Additional personal data processing

If we intend to process personal data for a purpose other than the original reason(s) for which we collected the personal data, we will inform you prior to that additional processing. We will provide you with information on the new purpose(s), and any further relevant information, to the extent that you do not already possess such information.

XI. Role as personal data Controller, Processor, or Sub-Processor

Depending upon the engagement and purpose of personal data processing, the Plan and its affiliates, as applicable, are either the "Controllers," "Processors," or, in some cases, "SubProcessors," as defined under the GDPR.

XII. Contact

Our address is 120 Fifth Avenue, Suite 2114, Pittsburgh, PA 15222. Our Data Protection Officer can be reached in writing at Highmark Health, Attn: Data Protection Officer, 120 Fifth Avenue, Suite 2114, Pittsburgh, PA 15222, or via email at privacyinternational@highmarkhealth.org.

Last revised: April 2021.