

**Highmark Health**  
**Information and Disclosures of Personal Data under the European Union General Data Protection Regulation (GDPR)**

The European Union's General Data Protection Regulation (GDPR) requires that personal data from the European Union (EU)/European Economic Area (EEA) is subject to special protection. The GDPR also provides EU-based individuals ("Data Subjects") with certain individual rights with respect to their personal information. These include:

1. **The right to be informed** about the collection and use of their personal data.
2. **The right of access** to find out what data is stored about them.
3. **The right to rectification** of their personal data if it is inaccurate or incomplete.
4. **The right to erasure** to enable an individual to request the deletion or removal of certain personal data where there is no compelling reason for its continued processing.
5. **The right to restrict processing** to 'block' or suppress processing of personal data.
6. **The right to data portability** allowing individuals to obtain and reuse their personal data for their own purposes.
7. **The right to object** to the processing of personal data under certain circumstances.
8. Various 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).

Highmark Health, including its affiliates and subsidiaries that it has identified as having GDPR compliance obligations, will make all reasonable efforts to abide by the GDPR and provide at least the same level of data protection for personal data received from the EU and processed, as the privacy protections set forth in our Notice of Privacy Practices (NPPs). We will also make reasonable attempts to accommodate requests by Data Subjects to exercise the rights listed above. Where necessary and appropriate we have implemented organizational and technical measures that include internal data protection policies and maintaining documentation on our processing activities. We have also appointed a Data Protection Officer.

In order to enable Data Subjects to exert their rights under the GDPR, we are making the following disclosures for data received directly from an individual and data received from third parties. For purposes of this disclosure document, references to “we”, “us” or “our” mean Highmark Health and its appropriate affiliates, and references to “you” and “your” mean the Data Subject.

### **1. How We Use Personal Data.**

We use Personal Data for purposes related to providing medical care and advice, as well as for insurance and health benefits administration purposes. We also use your Data for certain administrative and corporate services. The medical care services include but are not limited to: providing medical treatment, consulting with other providers of care and maintaining your medical records. Insurance and Plan Administration purposes include but are not limited to: enrolling members for coverage, processing claims, sending Explanations of Benefits, responding to your questions, providing care management and wellness services, helping you find care providers, notifying you of changes to benefits, reporting financial and other data to clients, and fraud prevention. Our administrative and corporate services include but are not limited to: accepting and processing applications for employment, keeping employment records, billing, and developing and marketing new products and services. Please review the applicable Notice of Privacy Practices for additional information.

### **2. Who Receives Personal Data?**

Members of our workforce, including medical providers, use Personal Data in order for us to provide services to you. In addition, we share Personal Data as necessary with certain third parties who contract with us to provide services. We also share Personal Data with clients, e.g. group health plans, and some of their vendors.

### **3. How long is Data stored?**

We store data for as long as is necessary to provide the services and for a reasonable retention period. Our usual storage period is seven (7) years, but legal requirements and our corporate policies might lead to longer or shorter periods.

#### **4. Your Rights with Respect to Your Personal Data.**

You have the right at any time to request access to and rectification or erasure of personal data that we hold. You can also request restriction of processing of your Personal Data, and you have the right to data portability. 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.

#### **5. Withdrawal of Consent**

We collect consent for processing of EU Personal Data. 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 processing of your withdrawal you must include your name, address, your Identification Number (if the withdrawal is directed to Highmark concerning your health insurance coverage) and the specific processes for which you no longer consent in your request. Withdrawing consent will not affect the lawfulness of processing that took place based on the consent you provided before the withdrawal.

#### **6. Complaints.**

You have the right to lodge a complaint with the appropriate data protection authority.

#### **7. Source of Data and Legal Basis for Our Data Processing**

In order to provide services to you, we receive Personal Data from you, from your providers of medical care, from your employer and from other third parties. We need access to your Personal Data, such as name, address and medical information, regardless of who provides it, in order for us to provide the services described above.

#### **8. Is Personal Data Used for automated decision-making or profiling?**

We use automated decision-making processes and profiling in the performance of our insurance and plan administration contracts. For example, claims processing is primarily an automated process. We also use profiling to identify individuals who would benefit

from care and case management, medication management and other programs offered as part of the health benefits contract . We also use profiling to identify opportunities for communication with you.

### **9. Location of Data Processing**

All Personal Data that we process is done so in the United States.

### **10. Additional Processing**

If we intend to use Personal Data for a purpose other than the original purposes for which we collected the Data (see Notice of Privacy Practices and Item 1. above), prior to that additional processing, we will provide you with information on that other purpose and any further relevant information, insofar as you do not already possess such information.

### **11. Processors and Controllers**

Depending upon the engagement and purpose Highmark Health and its Affiliates are either the Controllers, Data Processors and in some cases, Sub-Processors with respect to your Personal Data. Our address is 120 Fifth Avenue Place, Suite 2114, Pittsburgh, PA 15222.

Our Data Protection Officer can be reached at Highmark Health, 120 Fifth Avenue Place, Suite 2114, Pittsburgh, PA 15222 or via email at [privacyinternational@highmarkhealth.org](mailto:privacyinternational@highmarkhealth.org).