PURPOSE:
At Devoted Health, we are committed to maintaining the confidentiality of our members’ medical and financial information, which we refer to as “personal information”, regardless of format: oral, written, or electronic. This policy of privacy practices illustrates how we may collect, use and disclose personal information and our members’ rights regarding that information.

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Devoted Health must take measures to protect the privacy of personal information. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of personal information include member name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.

POLICY:
Devoted Health protects our members’ personal information in a variety of ways. For example, we authorize access to personal information by our employees and business associates only to the extent necessary to conduct our business of serving our members, such as paying claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of personal information for our members even if they no longer maintain coverage through us. We are required by law to:

- Protect the privacy of member personal information
- Provide detailed privacy policy explaining our duties and privacy practices regarding your personal information;
- Notify our Members following a breach of unsecured personal information; and
- Abide by the terms of within these guidelines
Collection of personal information
Devoted Health will collect most personal information directly from our members through the application process. We may also obtain our members’ personal information from third parties. These third parties may include producers, employers, health care providers, other health plans or insurers, and state and federal agencies.

Record Retention of Member information
Devoted Health, pursuant to CMS’ retention requirements will maintain all member records, transactions, and documents for 10 years from the end date of an MA contract or the completion date of an audit, whichever is later.

Use and disclosure of personal information
Devoted Health may use or disclose personal information without specific authorization from members for the purposes described below. For other purposes, Devoted Health will request specific authorization from our members in writing, electronically, or over the phone, which they may grant or reject. If granted, members can revoke the authorization at any time by informing Devoted Health in writing.

Purposes for which Devoted Health can use or disclose personal information without authorization:

● Treatment: Devoted Health may disclose personal information about members that physicians or other health care providers request in order to help with medical treatment or services.

● Payment: Devoted Health may use and disclose personal information in order to process medical claims.

● Health Care Operations: Devoted Health may use and disclose personal information for health plan operations (e.g. quality assessment and improvement activities, risk adjustment activities, engagement in care or case management, etc.)

● Business Associates: Devoted Health may disclose personal information to Business Associates. These are entities or individuals that are not employed by Devoted Health that perform healthcare operations on our behalf which require that the Business Associate create, receive, maintain, or transmit personal information. Devoted Health must have contracts with our business associates that require them to maintain the confidentiality of any personal information.

● Appointment/ Service Reminders: Devoted Health may use personal information to contact members for the purpose of reminding to obtain health services or to provide information on treatment alternatives and/or health-related products or services that may be of interest to our members or provided by Devoted Health, included in plan of benefits or otherwise valuable products or services that are only available to current members.

● Individuals involved in member’s care: Devoted Health may disclose personal information to a family member or other individuals who are directly involved in care or payment of care.

● As required by law: Devoted Health may use or disclose personal information when required by federal state or local law. For example Devoted Health may disclose personal information to a health oversight agency, to include the Secretary of the Department of Health and Human Services or a state insurance department, for activities such as audits, investigations or related to licensure.

● Public Health and Safety: Devoted Health may disclose personal information to the extent necessary to avert a serious and imminent threat to our members health or safety or the health or safety of others.
Health Insurance Portability and Accountability Act Policy

- Research: Devoted Health may disclose personal information as part of a limited data set for purposes of research, public health or healthcare operations. In addition Devoted may disclose personal information to researchers when their research has been approved by a review board that has reviewed the research proposal and established protocols to ensure the confidentiality of your personal information.
- Legal Proceedings: Devoted Health may disclose personal information in response to a court or administrative order, subpoena, discovery request, or other lawful process.
- Law Enforcement: Devoted Health may disclose personal information to law enforcement officials if we receive a court order, warrant, grand jury subpoena or inquiry for purposes of identifying or locating a suspect, fugitive, material witness or missing person.

Physical access to building
- Employees access office via a single main entrance or employee entrance with a badge
- Main entrance is locked after hours and is unlocked each morning at 7:30am

Security of electronic PHI (e-PHI)
- Employees whose job functions require access to our computer system will be given a secure, unique password to access the system. Access will be immediately terminated for employees upon separation of the company.

REFERENCED DOCUMENTATION:
N/A

REGULATORY REFERENCES:

ACRONYMS & DEFINITIONS:
HIPAA - Health Insurance Portability and Accountability Act of 1996
CMS - Centers for Medicare & Medicaid Services
MA - Medicare Advantage

REVIEW:

<table>
<thead>
<tr>
<th>Accountable for Policy Maintenance:</th>
<th>Kiley Cernansky</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable for Implementation:</td>
<td>Shannon O’Kane</td>
</tr>
</tbody>
</table>
## Health Insurance Portability and Accountability Act Policy

### Review and Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision #</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.01.2020</td>
<td>2.0</td>
<td>Updated policy and annual review of policy (Shannon O'Kane)</td>
</tr>
<tr>
<td>02.05.2021</td>
<td>2.1</td>
<td>Annual Review (Kiley Cernansky)</td>
</tr>
<tr>
<td>01.27.2022</td>
<td>2.3</td>
<td>Annual Review (Shannon O'Kane)</td>
</tr>
</tbody>
</table>