HIPAA PRIVACY/SECURITY ACTION PLAN

1. If you are a fully insured group health plan:

   - Determine if you are receiving protected health information other than summary health information and enrollment/termination information.

   - If you are receiving protected health information and will continue to receive it, see the steps listed below for self funded group health plans and fully insured group health plans receiving protected health information.

   - If you are not receiving protected health information, no further action is necessary.

2. If you are a self funded group health plan, or are a fully insured group health plan receiving protected health information other than summary health information and enrollment/termination information:

   - Select a Privacy Officer.


   - Determine appropriate and necessary changes based on Gap Analysis. See HIPAA Privacy/Security Reg Gap Analysis Decision Tree attached.

   - Document new privacy/security procedures.

   - Provide training on privacy/security procedures and HIPAA to all employees, including management.

   - Implement internal privacy/security changes.

   - Discuss necessary external changes with business partners and implement changes and/or business associate agreements.

   - Select a contact to handle privacy complaints and Privacy Notice questions and inquiries.

   - Select a contact to receive and implement a process for responding to requests for access to protected health information, requests to amend protected health information, requests to limit uses of protected health information, and requests for accountings of the use and disclosure of protected health information.

   - Publish Privacy Practices Notice and distribute by compliance date.

   - Amend Plan Documents of the group health plan.

   - Document all actions taken to comply. Refer to Requirements for Covered Entities – Documentation Requirements in the HIPAA Privacy Regulation Summary.

Additional steps will be necessary if the group health plan or employer is using protected health information for purposes other than treatment, payment or health care operations. In those cases implementation of processes relating to authorizations and tracking to provide a 6 year accounting of disclosures will be necessary.
HIPAA PRIVACY/SECURITY REG GAP ANALYSIS SURVEY

Please complete the questions below based on the following definition of Protected Health Information.

**Protected Health Information.** Information that identifies the individual, or could reasonably be used to identify the individual, and relates to a past, present, or future:
- physical or mental health condition;
- the provision of health care; or
- payment for health care.

Examples of information that may include protected health information are: Rx Drug Card statements; utilization reports; claim reports; case management reports; check registers and funding requests; out-of-contract payment requests; claim forms; EOB's; pre-existing, accident or subrogation correspondence; coverage determination inquiries; medical record requests, Attending Physician Statements; treatment plans; stop-loss claim filings and payments; 50% or large case notices; lists of lasered individuals; COBRA notices and payments; FMLA and USERRA records for the health plan; wellness program reports; EAP records; and FSA or flex records. NOTE: Protected Health Information does not include employer records that did originate or result from a health plan sponsored by the employer.

**Department/Person:**

**Do you or your department receive, use or send Protected Health Information as defined above?** □ Yes □ No

*If yes, complete the following questions:*

1. List the type of protected health information and how it used:

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>How Information is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Is the protected health information in electronic or paper format? □ Electronic □ Paper

3. How is the protected health information stored?

4. Is the protected health information disclosed to anyone else in the company? □ Yes □ No
   *If yes, please list the name/department and reason for disclosure:*

<table>
<thead>
<tr>
<th>Name/Department</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Is the protected health information disclosed to anyone outside the company? □ Yes □ No
   *If yes, please list below the name, address and reason for disclosure:*

<table>
<thead>
<tr>
<th>Company/Person</th>
<th>Address</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Provided for Informational Purposes by UMR.
HIPAA PRIVACY/SECURITY REG GAP ANALYSIS DECISION TREE

Does each employee receiving PHI need it?

If no, remove access or change to summary or de-identified information.

If yes, is PHI limited to minimum necessary?

If yes, document as ok.

If no, reduce to minimum necessary.

Is PHI adequately protected?

Is PHI in non-electronic formats adequately protected as required by Privacy Regs?

If no, determine appropriate protection and document policy.

If yes, document as ok and what policy is for protection.

Is PHI that is stored, received or sent electronically protected as required by the Security regs?

If no, implement appropriate protection and document policy.

If yes, document as ok and what policy is for protection.

Does each external person receiving PHI need it?

If no, reduce to minimum necessary.

If yes, is PHI limited to minimum necessary?

If yes, document as ok.

If no, determine appropriate protection and document policy.

Obtain Business Associate Agreement.