HIPAA CHECKLIST

The following checklist is designed to assist you in determining your legal obligations and the applicable compliance deadline for the federal privacy rules, which are part of the Health Insurance Portability and Accountability Act.

1. Determine if your company must comply with the HIPAA privacy rules

a. What type of health plans (Plans) do you offer employees?
{Each of these Plans is potentially covered}

- ☐ Medical and health plans
- ☐ Dental plans
- ☐ Vision plans
- ☐ Flexible Spending Account plans (FSA)

b. What type of Plans, and the documents generated or received in connection with the Plans that reflect an employee's health or medical condition, are excluded from HIPAA coverage?

- ✓Workers' compensation
- ✓Life and accidental death insurance plans
- ✓Disability insurance plans
- ✓FMLA forms and certifications, and other employment related documents

c. **Caution:** Even if HIPAA does not apply to your business, the medical records/confidentiality rules, which are part of the Americans with Disabilities Act (ADA), require all employers with more than 15 employees to maintain all medical information on employees in restricted, confidential medical files, which are separate from the general personnel files on employees. This includes all of the documents generated or maintained under any of the excluded plans listed above. ***Nothing in HIPAA reduces existing obligations imposed on employers under the ADA to maintain the confidentiality of an employee's medical information.***

d. Are any of your Plans self-administered?

- ☐ Do you use a third-party administrator on claims? If so, the plan is not "self-administered"
- ☐ Identify number of participants in each self-administered Plan. ***If less than 50 then the Plan is not covered by HIPAA's privacy rules***

e. If the Plan is fully insured, do you receive PHI on employees? If you receive only Summary Health Information and enrollment/disenrollment information, you do not have to comply with the privacy rules with respect to that Plan.

f. **Caution**: Even if HIPAA's privacy rules do not apply to your Plans, an employer's right to obtain personal medical information on an employee is regulated by HIPAA. For example, an employer cannot require an employee to waive his rights under the privacy rules and can't retaliate against an employee for asserting rights under the privacy rules. You may still require an employee to provide medical information to support a request for FMLA or a request for accommodation under the ADA.

2. **Determine compliance deadline.** If you have a Plan that is covered then you must be in compliance no later than April 14, 2004. Large plans, which had $5 million or more in gross receipts, were to be in compliance by April 14, 2003; all other plans must be in compliance by 2004. ☐

3. **What is Protected Health Information (PHI)?** PHI is individually identifiable health information related to the individual's past, present or future physical or mental health.

4. **If HIPAA applies, then you must adopt and implement a comprehensive Privacy Plan and set of policies and procedures** to comply with restrictions on use/disclosure of PHI in compliance with the privacy rules. There are several components of this type of Privacy Plan.

   a. **A company officer must be designated as Privacy Official.** This person will be responsible for developing/implementing policies and procedures. ☐
   b. **Implement safeguards** to protect PHI from intentional or accidental disclosure (administrative, technical and physical). ☐
   c. **Identify likely uses/disclosures of PHI** for purposes other than treatment, payment and operations; prepare authorizations for each. ☐
   d. **Prepare and distribute Notice of Privacy Practices**; include summary of individuals' rights and (if applicable) a statement noting that the Plan may/will disclose PHI to the Plan Sponsor. ☐
   e. **Provide complaint mechanism** for individuals to challenge use/disclosure of PHI; designate contact person for receiving complaints. ☐
   f. **Establish sanctions** for employees or business associates who violate policies/procedures. ☐
   g. **Provide privacy training** program for employees; document training. ☐

5. **Don't require individual employees to waive privacy rights** as a condition of enrollment, eligibility, treatment or payment in the Plan. ☐

6. **Maintain documentation**; required to provide accounting for 6 years. ☐

7. **Amend plan documents** to recite permitted and required uses and disclosures of PHI; Sponsor must provide certification to Plan that the documents have been amended. ☐

8. **Review relationships** with entities/persons that receive PHI from the Plan; prepare business associate agreements for each. ☐

After HIPAA, How Can An Employer Obtain PHI?

1. **Employee may authorize** the disclosure (see sample authorization attached). ☐

2. **PHI may be "de-identified."** ☐

3. **Summary Health Information may be disclosed** for employer to use in obtaining premium bids or amending or terminating a plan. ☐

4. **Information may be disclosed in "limited data set"** for health care operations. Plan and recipient must enter into a data use agreement (like a BA agreement). ☐

5. **Amendments to Plan documents**

   a. Have Plan documents been amended to identify and/or provide:

      i. The permitted and required uses and disclosures of PHI ☐

      ii. Who, by name, title or functional role is designated to received and have access to PHI and the fact that access is limited to only those individuals ☐

      iii. Sponsor has established appropriate sanctions for employees who fail to comply with privacy requirements ☐

      iv. Specific plan administrative functions for which the Sponsor is requesting the PHI be disclosed ☐

   b. Does the certification of the Plan document amendment provide that:

      i. Plan Sponsor agrees not to use or further disclose the PHI received ☐

      ii. Plan Sponsor has established a mechanism to require any agents or subcontractors with which it shares PHI received from the Plan to the same restrictions/conditions as the Sponsor with respect to such PHI ☐

      iii. Plan Sponsor won't use disclosed PHI to make employment-related decisions or take employment-related actions or make decisions regarding any other benefit or employee benefit plan the Sponsor offers/proposes ☐

      iv. Plan Sponsor has established and identified a policy and procedure to report to the Plan any use or disclosure that does not comply with these requirements of which it becomes aware ☐

      v. Sponsor will make PHI available for amendment and incorporate any ☐

appropriate amendments to PHI. Sponsor will identify parameters under which it will deny access or amendments/corrections

vi. Sponsor will provide accurate accounting related to whom the PHI was disclosed, when and for what purpose ☐

vii. Sponsor has established a policy and procedure to make its internal practices, books and records relating to use and disclosure of PHI available to DHHS in order to determine compliance ☐

viii. Sponsor will not maintain or retain in any form copies of PHI when no longer needed for the purpose for which disclosure was made ☐

ix. **Caution:** Very similar to business associate (BA) agreements except that there are TWO modes of enforcement: violation of HIPAA and ERISA

Authorization for Release of Protected Health Information

Employee Name: _____

SECTION A

(Must be completed for all Authorizations)

1. I hereby authorize the use or disclosure of my individually identifiable protected health information ("**Information**") as described below. I understand and agree that this Authorization is voluntary. I understand that if the organization authorized to receive the Information is not a health plan or health care plan covered by federal privacy regulations, the released Information may no longer be protected from further use or disclosure by federal privacy regulations.

Specific description of Information covered by the Authorization (including date(s)):

_____
_____
_____

Persons/organizations authorized to make the disclosure or use of the Information:

_____
_____
_____

Persons/organizations to whom disclosure of the Information is to be made:

_____
_____
_____

2. The employee or the employee's representative must read and initial the following statements:

   a. I understand that [plan name] will not condition my enrollment, eligibility, treatment, or payment in the [plan name] on my providing this Authorization.

Initials: _____

b. I understand that I may see and receive a copy of the Information described on this Authorization if I request it in writing, and that I will receive a copy of this Authorization after I sign it. I further understand that under Virginia law, this information will be provided to me within 15 days of such written request and that a reasonable charge may be made for the service of maintaining, reviewing and preparing such copies.

Initials:_____

c. I understand that I have the right to refuse to sign this Authorization.

Initials:_____

d. I understand that this Authorization will expire on __/__/___

Initials:_____

e. I understand that I may revoke this Authorization at any time by notifying [plan name] in writing, except to the extent [plan name] has taken action in reliance on this Authorization.

Initials:_____

f. I understand that if the organization authorized to receive the Information is not a health plan or a health care plan covered by federal privacy regulations, the released Information may no longer be protected from further use or disclosure by federal privacy regulations and may be subject to redisclosure.

Initials:_____

g. I acknowledge that I have received a copy of this Authorization.

Initials:_____

SECTION B

(Must be completed only if [plan name] has requested the Authorization for its own purposes or for use or disclosure by another plan or a health plan)

1. The specific purpose(s) for which the Information is requested are:

_____

2. [Plan name] will [ ] will not [ ] receive financial or in-kind compensation in exchange for using or disclosing the Information.

Signature of employee or employee's representative:_____ Date: _____ Time: ____

Printed name of employee's representative: _____

Relationship of employee's representative to employee:_____

Evidence of the authority of the employee's representative (attach evidence to last page of this Authorization): _____