

HIPAA COMPLIANCE WORKSHEET

This HIPAA Compliance Worksheet is designed to assist you in becoming compliant with the privacy requirements of HIPAA. As an employer offering a Health Flexible Spending Account, you are responsible for determining whether you are handling PHI (protected health information) and taking steps required by the Act to protect such information and the privacy of your plan participants. This worksheet is designed to provide a general guideline of the activities and procedures a plan sponsor should perform and the information is provided as a general guide for compliance. Following this checklist may or may not put you into compliance with HIPAA. Because each employer has distinct plan offerings, we recommend you have your HIPAA Compliance Plan reviewed by legal counsel, or to receive a legal evaluation proposal, see [Compliance review proposal](#).

- I. What benefit plans do you have that may be subject to the HIPAA privacy requirements?
- a. See Benefit Plans Table [Benefit Plan Table](#)
 - b. Do any of your plans require you to have procedures in place for HIPAA privacy requirements? List those plans here:

- II. As a plan sponsor, are you having to handle, receive or transfer any PHI (Protected Health Information)? Yes No

If yes, see the General Administrative Guidelines at http://www.eflexgroup.com/hipaa/hipaa_pg2.asp

If no, proceed with this worksheet.

See the training presentation <training presentation> for more information on PHI.

- III. Who will you designate as your Privacy Officer?

_____ (Name)

See the training presentation <training presentation> for more information on PHI.

IV. Do you have a Privacy Policy developed and communicated to staff? See http://www.eflexgroup.com/hipaa/gen_hip.pdf for a sample policy.

Completed: _____ (date)

V. Do you have a Notice of Privacy Practices developed and distributed to plan participants? You have a duty to advise the plan participants, including employees, spouses and adult dependents what their rights are under HIPAA. This is best done by mailing the Privacy Notice addresses to the employee, spouse and dependents. The notice may be done electronically as long as there is a process in place to ensure that those without access to e-mail, and spouses and adult dependents, are receiving the notice. See http://www.eflexgroup.com/hipaa/pn_flex.pdf for a sample Notice of Privacy Practices.

Completed: _____ (date)

Would you like eflexgroup to complete the mailing of the Notice of Privacy Procedures on your behalf? Click here to review our Privacy Notice service area and fees. [<Privacy Notice Page>](#)

VI. Do you have service advisors, third party administrators or individuals handling your flex plan administration? If so, you must provide them with a Business Associate Agreement that both you and your administrator must sign. See <http://www.eflexgroup.com/hipaa/baa.pdf> for a sample agreement.

Completed: _____ (date)

VII. Get training for appropriate staff to become aware of your duties under the Act as a plan sponsor and of your duties to your employees and plan participants. See <training powerpoint presentation> as one training resource, and document attendance and completion of training.

Completed: _____ (date)

VIII. Audit your HIPAA Compliance and document your compliance efforts. This means you should review the HIPAA Compliance Checklist and Worksheet periodically to determine whether you are handling any PHI, and whether you are providing proper notification of your policies.

After you have completed the above 8 steps, file this checklist along with signed copies of all Business Associate Agreements, a copy of your Notice of Privacy Practices and a listing of all employees, spouses and adult dependents to whom you mailed the Notice, the date of the mailing and the person responsible for the mailing, and a copy of your Privacy Policy.