

HIPAA Security Compliance

April 20, 2006 is the small plan compliance date for the security portion of the Health Insurance Portability and Accountability Act (HIPAA) that now extends to electronically transmitted or maintained Protected Health Information (e-PHI). Employers who sponsor group health plans are required to comply with this latest edition of HIPAA. The good news is if you sponsor a fully insured health plan and do not have access to your employee's PHI and/or e-PHI, you will only have a few steps to take.

WHAT YOU SHOULD DO

As we reported to you in 2003 when the Privacy requirements of HIPAA became effective, we believe that most of our clients sponsor plans that are fully insured. The issue is whether you are a "Hands-Off" plan sponsor and have no access to PHI or e-PHI. A group health plan that does not create, receive, or maintain PHI or e-PHI is Hands-Off. The Conestoga Group provides the Health Advocate Service to allow a plan sponsor to remain Hands-Off while still providing a service to satisfy employee healthcare assistance needs. If you are Hands-Off, your active compliance requirements are limited to numbers 1 – 4 below. If your Company is NOT Hands-Off you will need to complete all 7 tasks. If your Company also has a Health FSA please make sure you review the Health FSA section on page 2 for additional compliance requirements.

- 1. Business Associate Agreements** – Update with required security language. (The Conestoga Group will be sending under separate cover a revised Business Associate Agreement with the security language to all clients who purchase medical, dental or prescription benefits through The Conestoga Group).
- 2. Designate a Security Official** – This will be an additional responsibility given to an employee who has other duties.
- 3. Risk Analysis Documentation** – A Covered Entity should assess its existing policies, procedures and practices for creating, maintaining, using and disclosing e-PHI to determine whether there are gaps between the Covered Entity's current status and the Security Rules' security standards. This "gap" assessment will be the roadmap for a Covered Entity's remedial efforts. Included with this package is a Risk Analysis Worksheet you may use.
- 4. Policies & Procedures** – Even employers that are "Hands-Off" PHI will still need a simple Security Policy in place. Attachment II of this document is a sample policy, which you may use as a starting point for your own.
****STEPS 5, 6 and 7 Only for Plans that are NOT Hands-Off****
- 5. Plan Amendment** – If an employer wishes to receive PHI and e-PHI from the group health plan they must have their plan document amended to ensure they will establish the proper security measures to comply with HIPAA Security. (This would be for a plan sponsor who is NOT Hands-Off PHI).
- 6. Risk Management** – Once the risk analysis has been performed, the Covered Entity must document their findings and develop a program to address all of the security risks and vulnerabilities identified and should then document the actions that were undertaken to comply with the security rule.
- 7. Periodic Evaluation** – A periodic evaluation should be done on the risk management procedures in place to confirm the current policies and procedures continue to meet the requirements of the security rules.

HEALTH FSA'S

Plan sponsors with Medical Flexible Spending Accounts (FSAs) must treat the FSA as an additional, separate covered plan and meet separate compliance requirements. Below are the three scenarios we are aware of.

MEDICAL FSA SELF-ADMINISTERED WITH LESS THAN 50 ELIGIBLE EMPLOYEES

- No additional compliance requirements

MEDICAL FSA SELF-ADMINISTERED WITH MORE THAN 50 ELIGIBLE EMPLOYEES

- Full compliance

MEDICAL FSA ADMINISTERED BY INDEPENDENT TPA WITH ANY # OF EMPLOYEES

- Full compliance required by employer, however your TPA may provide compliance materials to assist you.

NOTE:

If you have a Medical FSA that is either self-administered with more than 50 eligible employees or administered by an independent TPA you were required to do full privacy compliance for this plan in 2004. This process was outlined in a letter from The Conestoga Group on 4/1/04. If you completed those requirements in 2004 you will need to update your current BAA with the vendor by adding the security language to the BAA and create a security policy for the plan. Some vendors have mailed the BAA language directly to their clients. If you are unsure if your BAA has the security language or if you need assistance with the security policy you may contact the vendor directly or contact Fredonna Smith of The Conestoga Group for assistance.

PENALTIES FOR FAILURE TO COMPLY

Under HIPAA, the penalties for noncompliance with the Security Rules are up to \$100 per violation but not more than \$25,000 per year for all violations of an identical requirement or prohibition. Judgments rendered through the courts are additional potential costs.

WHEN TO SEEK HELP

If you have any questions regarding the applicability of HIPAA Security laws relative to any benefit plans or procedures you currently have in place, we strongly urge you to discuss these issues with the vendors you currently use. If you have implemented these plans through our office, please contact us for explanations. If you are an employer who may receive PHI or e-PHI, we would suggest you consult with legal counsel to determine how to best establish the proper procedures and policies. It must be emphasized that this Legislative Update does not take into consideration any specific factors that may be unique to your situation.

If you wish to review our other publications on The Health Insurance Portability and Accountability Act (HIPAA) regarding HIPAA Privacy or HIPAA Special Enrollment Rights, please visit our Client Community website located at www.conestoga.clientcommunity.com. Your ID is your full e-mail address and your password is Conestoga. Once you log onto the site, click on News and scroll down to the publication you wish to review.

The Conestoga Group is an insurance, investment and employee benefits broker and consulting firm based in Frazer, PA. Conestoga specializes in providing financial products and services to small businesses and their owner/executives and other employees. Founder and President Brad Palmer is an Investment Advisory Representative of Commonwealth Financial Network-a registered investment advisor and member firm of the NASD/SIPC. Brad can be reached at 610-889-9500 extension 101 or at brad.palmer@conestoga.biz.

NOTICE

These legislative descriptions are our interpretations of information provided to us by various legal and other resources as of 3/23/06. It is possible the information was presented incorrectly or that we have misunderstood the presentation. The purpose of this communication is to provide you with basic summary information on the subject matter and assist you in determining whether or not you may need to seek further legal or other assistance. This communication should not be construed as legal, tax, investment, or other advice and does not take into consideration any specific factors that may be unique to the reader's situation.

Attachment I Risk Analysis Worksheet

	YES	NO	N/A
1. Is your medical plan fully insured?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Is your dental plan fully insured?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Is your prescription plan fully insured?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Do all employees route all benefit related questions regarding personal health information to Health Advocate for assistance?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Does your company have a written HIPAA Security Policy? (See Attachment II attached for example to prepare policy)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Do you offer a Medical FSA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Is your Medical FSA self-administered? *If no go to section below labeled "For Plan Sponsors With Medical FSAs"	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. If yes to 6 & 7 does Company have less than 50 benefit eligible employees? **If no go to section below labeled "For Plan Sponsors With Medical FSAs."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If yes to questions 1-5 and no to 6, **or** yes to all questions, Security Officer should sign below and store this document with Company HIPAA Privacy and Security Policies.

Signed: _____ Date: _____
Security Officer

For Plan Sponsors With Medical FSAs:

***** If you use an independent TPA, regardless of the number of benefit eligible employees full compliance is required. The TPA would have been required to take the necessary steps to safeguard your employees's health information. At a minimum you should make sure your BAA with the TPA has been updated to include the required Security language, have a security policy in place and confirm your TPA has made the necessary compliance updates.

Compliance process has been completed with TPA and yes to questions 1-5 above. Security Officer should sign below and store this document with Company HIPAA Privacy and Security Policies

Signed: _____ Date: _____
Security Officer

****** If you self-administer a Health FSA for a plan with over 50 benefit eligible employees, full HIPAA compliance is required by your plan. You should consult legal counsel to confirm the Company is in compliance with all requirements

Full compliance process completed for self-administered Health FSA with over 50 benefit eligible employees and yes to questions 1-5 above. Security Officer should sign below and store this document with Company HIPAA Privacy and Security Policies

Signed: _____ Date: _____
Security Officer

Attachment II

Sample HIPAA Security Policy

For Fully- Insured Plan With No Access to PHI

Caution: This sample document is for a hypothetical covered entity and it may not apply to your factual situation. It is provided here for illustrative purposes only, and it may not be used "as it" for any purpose. If you wish to use this sample as a starting point for you own document, advice of legal counsel is required.

Introduction

The [Company Name]_____ sponsors a group health plan(the Plan) of which all of the benefits are provided under contracts with one or more health insurers (collectively, the Insurer). Neither the Company nor any member of its workforce creates, receives, maintains, or transmits electronic protected health information (as defined below) on behalf of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations require the Plan to implement various security measures with respect to electronic protected health information.

Electronic protected health information (e-PHI) is protected health information that is transmitted by or maintained in electronic media. Protected health information (PHI) is the information that is subject to and defined in the Plan's privacy policies and procedures. For purposes of the Policy, PHI does not include (1) summary health information for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Plan; (2) enrollment and disenrollment information; and (3) information received pursuant to a HIPAA-compliant authorization. (These three types of information are referred to as Exempt Information).

Electronic Media means:

1. Electronic storage media means electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card.
2. Transmission media used to exchange information already in electronic storage media (e.g., internet, extranet, leased lines, dial-up lines, private networks. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

It is the Plan's policy to comply fully with HIPAA's requirements.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. This Policy does not address requirements under federal laws other than HIPAA or under state laws.

I. Security Official

[Name of employee and title] is the Security Official for the Plan. The Security Official is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy.

II. Risk Analysis

The Plan has no employees. Except for functions performed by the Company using Exempt Information, all of the Plan's functions, including creating and maintenance of its records, are carried out by the Insurer. The Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Insurer. Accordingly, the Insurer creates and maintains all of the electronic PHI relating to the Plan, owns or controls all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and has control of its employees, agents, and subcontractors that have access to electronic PHI relating to the Plan. The Plan has no ability to assess or modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan—that ability lies solely with the Insurer.

Because the Plan has no access to or control over the Insurer's employees, equipment, media, facilities, policies, procedures, or documentation affecting the security of electronic PHI relating to the Plan, and the Insurer is a covered entity that is responsible under HIPAA to implement security measures with respect to electronic PHI (including electronic PHI relating to the Plan), the Plan's policies and procedures (including this policy) do not address the following standards (including the implementation specifications associated with them) established under HIPAA and set out in Subpart C of 45 CFR Part 164:

- Security management process; workforce security, information access management; security awareness and training; security incident procedures; contingency plan; evaluation; business associate contracts and other arrangements; facility access controls; workstation use; workstation security; device and media controls; access control; audit control; integrity; person or entity authentication; and transmission security.

Because the Company has no access to electronic PHI relating to the Plan, the Plan is not required to include provisions regarding security in its plan document.

III. Documentation

Except to the extent controlled by the Insurer, the Plan's security policies and procedures shall be documented, reviewed periodically, updated as necessary in response to environmental or operational changes affecting the security of Plan electronic PHI, and any changes to policies or procedures will be documented promptly. Except to the extent controlled by the Insurer, the Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented. Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form and will be maintained for at least six years from the date of creation or the date last in effect, whichever is later. The Plan will make its policies, procedures, and other documentation available to the Security Official, the Insurer, and the Company, as well as other persons responsible for implementing the procedures to which the documentation pertains.