

HIPAA’S IMPACT ON EMPLOYERS

Summary Guide

Employer sponsored group health plans are considered covered entities under HIPAA’s Privacy Rule and as such, must comply with the requirements of the regulation in the same way health insurers and providers must comply. Use the information below as a quick reference to ensure your company’s group health plan is in compliance. *(A group health plan is not subject to the HIPAA requirements if, and only if, it is fully insured and does not create or receive PHI.)*

Remember, under HIPAA, there are two components of an employer – the group health plan and the plan sponsor. HIPAA regulations may vary for your company depending on which component wishes to receive PHI.

| GROUP HEALTH PLANS <i>(Employees who administer health benefits on behalf of employer)</i> | | | |
|--|--------------------------------------|-------------------------------------|---|
| TYPE OF FUNDING | RECEIVE Personal Health Info. (PHI)? | RECEIVE Summary Health Info. (SHI)? | PRIVACY REQUIREMENTS |
| Fully Insured | √ No | √ Yes | <ol style="list-style-type: none"> 1. Refrain from interfering with employees exercising their rights under the Privacy Rule (e.g., requesting access to or a copy of their health information, filing a privacy complaint); and 2. Refrain from requiring any person to waive rights under the Privacy Rule as a condition of receiving payment, enrolling in a health plan or being eligible for benefits. |
| Self-Insured OR Cost-Plus | √ Yes | √ Yes | <ol style="list-style-type: none"> 1. Refrain from interfering with employees exercising their rights under the Privacy Rule (e.g., requesting access to or a copy of their health information, filing a privacy complaint); 2. Refrain from requiring any person to waive rights under the Privacy Rule as a condition of receiving payment, enrolling in a health plan or being eligible for benefits; 3. Designate a privacy official who is responsible for the development and implementation of the group health plan’s policies and procedures; 4. Designate a contact person (or office) who is responsible for receiving complaints filed under the Privacy Rule; 5. Establish policies and procedures concerning PHI that comply with the Privacy Rule; 6. Train all members of the workforce on the group health plan’s PHI policies and procedures; 7. Establish appropriate administrative, technical, and physical safeguards to protect the privacy of PHI from intentional or unintentional use or disclosure that violates the Privacy Rule; 8. Provide a process for individuals to make complaints concerning the group health plan’s policies and procedures, or its compliance with its policies and procedures, or the Privacy Rule; 9. Establish and apply appropriate disciplinary measures against members of its workforce for violations of the group health plan’s policies and procedures, or the Privacy Rule; 10. Act promptly to correct a violation or otherwise lessen the harmful effects resulting from a violation of its policies and procedures about which it has knowledge; 11. Provide Notice of Privacy Practices to members of the group health plan; and 12. Send agreements to business associates to ensure HIPAA compliance dealing with PHI. |

PLAN SPONSORS (Employers)

| TYPE OF FUNDING | RECEIVE Personal Health Info (PHI)? | RECEIVE Summary Health Info (SHI)? | PRIVACY REQUIREMENTS |
|--|-------------------------------------|------------------------------------|---|
| Fully Insured OR Self-Insured OR Cost-Plus | √ No | √ No | The plan sponsor has no compliance obligations. |
| Fully Insured OR Self-Insured OR Cost-Plus | √ No | √ Yes | SHI may be released to a plan sponsor if the plan sponsor agrees to only use the information to obtain premium bids for providing health insurance coverage to the group health plan, or to modify, amend or terminate the group health plan. |
| Fully Insured OR Self-Insured OR Cost-Plus | √ Yes | √ Yes | <p>Prior to any release of PHI to a plan sponsor, the plan sponsor must provide certification to the group health plan that the plan documents have been amended to incorporate the following provisions:</p> <ol style="list-style-type: none"> 1. Only disclose PHI as permitted by the plan documents or as required by law; 2. Not use or disclose the PHI for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the sponsor; 3. Ensure "adequate separation" of records and employees is established and maintained between the group health plan and the plan sponsor; 4. Ensure agents and subcontractors (e.g., benefits consultants) agree to abide by the same restrictions and conditions as the plan sponsor in regard to the use of PHI received from the group health plan; 5. Report any improper use or disclosure of PHI to the group health plan; 6. Allow individuals to inspect and obtain copies of PHI about themselves; 7. Allow individuals to request to amend PHI about themselves; 8. Provide individuals with an accounting of disclosures of PHI made within the six years prior to the request for such accounting; 9. Return or destroy PHI provided by the group health plan that is still maintained by the plan sponsor when no longer needed for purpose the disclosure was made. If not feasible, then limit the use and disclosure to those purposes; and 10. Make its internal practices, books and records relating to the use and disclosure of PHI available to the Dept. of Health and Human Services (HHS) for purposes of auditing the group health plan's compliance with the Privacy Rule. |

CareFirst BlueCross BlueShield has examined how HIPAA regulations will affect our business relationships with our customers. We are implementing policies and procedures that will both ensure our compliance and minimize disruption to the service you and your employees enjoy from us. **Please refer to the HIPAA Booklet, *HIPAA and Group Health Plans*, for more information on your relationship with CareFirst BlueCross BlueShield under HIPAA.**

These guidelines are provided as an informational service only. This not intended to replace or serve as legal counsel. To ensure that you and/or your company are taking the necessary steps to comply with HIPAA, you should consult your attorney.