

ATTACHMENT 4

EXTRACT OF SECTION 164.504 (f) OF THE PRIVACY REGULATIONS TO INCLUDE AN EXEMPLAR COMPLIANCE CHECKLIST FOR AMENDMENTS TO PLAN DOCUMENTS

Requirements for group health plans...[with some exceptions as noted in the regulation]...a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of:

- (A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or
- (B) Modifying, amending, or terminating the group health plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

- (i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart. Checklist item: Have the plan documents been amended to note the permitted and required uses and disclosures of protected health information? Are the listed provisions consistent with the HIPAA requirements?
- (ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to: [Checklist item: Obtain a copy of the certification of plan document amendment. Are each of the requirements below addressed in the certification?]
 - (A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law; Checklist item: Does the Plan Sponsor agree not to use or further disclose the disclosed information as stated above?
 - (B) Ensure that any agents, including a subcontractor, to who it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; Checklist item: Has the Plan Sponsor established a mechanism to require any agents or subcontractors with

which it shares PHI received from the Group Health Plan to the same restrictions and conditions as the Plan Sponsor with respect to such information?

- (C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or in connection with any other benefit or employee benefit plan of the plan sponsor; Checklist item: Do plan documents contain provisions that the Plan Sponsor will not use the disclosed protected health information to make employment-related decisions or take employment-related actions or make decisions regarding any other benefit or employee benefit plan the Plan Sponsor offers or proposes?
- (D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware; Checklist item: Has the Plan Sponsor established and identified a policy and procedure to report to the Group Health Plan any use or disclosure that does not comply with these requirements of which it becomes aware?
- (E) Make available protected health information in accordance with §164.524; Checklist item: Is there evidence that when individuals exercise their rights to an accounting of disclosures, the Plan Sponsor will make available to the Group Health Plan the PHI necessary to complete a designated record set?
- (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526; Checklist item: Is there evidence that when individuals exercise their rights to amend or correct protected health information contained in a designated record set, the Plan Sponsor will make available to the Group Health Plan the PHI necessary for the amendment and incorporate any amendments or corrections? Is there evidence that that the Plan Sponsor has identified the parameters under which it will deny access or amendments/corrections?
- (G) Make available the information required to provide an accounting of disclosures in accordance with §164.528; Checklist item: Has evidence been provided that the Plan Sponsor will provide information related to whom the PHI was disclosed, when and for what purpose?
- (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance with this subpart; Checklist item: Has evidence been provided that the Plan Sponsor has established a policy and procedure to make its internal practices, books and records relating the use and disclosure of PHI upon request by the Secretary of HHS (or authorized representative) in order to determine the Plan Sponsor's compliance?

- (I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which the disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; Checklist item: Has evidence been provided as to what the Plan Sponsor will do with the disclosed PHI once the purpose has been fulfilled or the task has been completed? What mechanism has been put into place to validate this has been done?
And
- (J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established. Checklist item: Do the plan documents and agreement clearly indicate a distinct separation between the employer (Plan Sponsor) and the health benefits administrator (Group Health Plan) that will have access to PHI?
- (iii) Provide for adequate separation between the group health plan and the plan sponsor. The Plan documents must : [Checklist item: Have the Plan documents been modified to meeting the following:]
- (A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee who receives the protected health information relating to payment, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description; Checklist item: Have plan documents been modified to describe who by name, title or functional role the employer, as the Plan Sponsor designates is the recipient and has access to the disclosed personal health information?
- (B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; Checklist item: Does the Plan document state that access to the disclosed PHI is restricted or limited to only those individuals as noted above?
- (C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph. Checklist item: Does the Plan document indicate that that Plan Sponsor has established appropriate disciplinary and corrective actions for employees who fail to comply with the privacy requirements?
- (3) *Implementation specifications. Uses and disclosures.*. A group health plan may:
- (i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of (f)(2) of this section; Checklist item: Does the

agreement list the specific plan administrative functions for which the plan sponsor is requesting the protected health information be disclosed?

- (ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph; Checklist item: Do any of the planned uses of the disclosed protection information to be shared with the Plan Sponsor deviate from the regulatory “allowed purposes?”
- (iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor unless otherwise permitted by this paragraph unless a statement required by §164.520 (b)(1)(iii)(C) is included in the appropriate notice; Checklist item: Does the agreement note that the Plan Sponsor has a privacy notice that includes a statement or statements noting that the Group Health Plan or the health insurance issuer or HMO may disclose or will disclose protected health information to the Plan Sponsor? ; and
- (iv) Not disclose protected health information to the plan sponsor for the purposes of employment-related actions or decisions in connection with any other benefit or employee benefit plan of the plan sponsor. Checklist item: Does the contract contain provisions that the Plan Sponsor will not use the disclosed protected health information to make employment-related decisions or take employment-related actions or make decisions regarding any other benefit or employee benefit plan the Plan Sponsor offers or proposes?

Exemplar Compliance Checklist

Health plans must review the certification from the plan sponsors that the plan documents have been amended to note the permitted and required uses and disclosures of protected health information and insure the amendments are consistent with the HIPAA requirements. Health plans should obtain a copy of the certification of the plan document amendments to ensure that all of the requirements listed below are addressed in the certification.

- Does the Plan Sponsor agree not to use or further disclose the disclosed information as stated above?
- Has the Plan Sponsor established a mechanism to require any agents or subcontractors with which it shares PHI received from the Group Health Plan to the same restrictions and conditions as the Plan Sponsor with respect to such information?
- Do plan documents contain provisions that the Plan Sponsor will not use the disclosed protected health information to make employment-related decisions or take employment-related actions or make decisions regarding any other benefit or employee benefit plan the Plan Sponsor offers or proposes?

- *Has the Plan Sponsor established and identified a policy and procedure to report to the Group Health Plan any use or disclosure that does not comply with these requirements of which it becomes aware?*
- Is there evidence that when individuals exercise their rights to an accounting of disclosures, the Plan Sponsor will make available to the Group Health Plan the PHI necessary to complete a designated record set?
- Is there evidence that when individuals exercise their rights to amend or correct protected health information contained in a designated record set, the Plan Sponsor will make available to the Group Health Plan the PHI necessary for the amendment and incorporate any amendments or corrections?
Is there evidence that that the Plan Sponsor has identified the parameters under which it will deny access or amendments/corrections?
- Has evidence been provided that the Plan Sponsor will provide information related to whom the PHI was disclosed, when and for what purpose?
- Has evidence been provided that the Plan Sponsor has established a policy and procedure to make its internal practices, books and records relating the use and disclosure of PHI upon request by the Secretary of HHS (or authorized representative) in order to determine the Plan Sponsor's compliance?
- Has evidence been provided as to what the Plan Sponsor will do with the disclosed PHI once the purpose has been fulfilled or the task has been completed? What mechanism has been put into place to validate this has been done?
- Do the plan documents and agreement clearly indicate a distinct separation between the employer (Plan Sponsor) and the health benefits administrator (Group Health Plan) that will have access to PHI?
- Have the Plan documents been modified to meeting the following:
 - ◆ to describe who by name, title or functional role the employer, as the Plan Sponsor designates is the recipient and has access to the disclosed personal health information?
 - ◆ to state that access to the disclosed PHI is restricted or limited to only those individuals as noted above?
 - ◆ to indicate that that Plan Sponsor has established appropriate disciplinary and corrective actions for employees who fail to comply with the privacy requirements?
- Does the contract agreement list the specific plan administrative functions for which the plan sponsor is requesting the protected health information be disclosed?

- Do any of the planned uses of the disclosed protection information to be shared with the Plan Sponsor deviate from the regulatory “allowed purposes?”
- Does the agreement note that the Plan Sponsor has a privacy notice that includes a statement or statements noting that the Group Health Plan or the health insurance issuer or HMO may disclose or will disclose protected health information to the Plan Sponsor?
- Does the contract or an amendment contain provisions that the Plan Sponsor will not use the disclosed protected health information to make employment-related decisions or take employment-related actions or make decisions regarding any other benefit or employee benefit plan the Plan Sponsor offers or proposes?