HIPAA Privacy Compliance Checklist

Task	Tasks Assigned to	Status/Work Performed
Obtain Education on HIPAA Privacy Requirements		
1. HIPAA EDI requirements.		
2. HIPAA privacy requirements.		
Organize the HIPAA Privacy Team and Create a Game Plan		
1. Obtain requisite board and management approval to develop HIPAA implementation team and plan.		
2. Establish a privacy budget.		
3. Assemble the HIPAA privacy team. • identify all departments that should be represented (e.g., HR, benefits, accounting, information systems, legal, etc.) • identify individuals from each department to be part of privacy team.		
4. Appoint a privacy officer.		
5. Establish internal timeline and meeting schedule		
Assess the Way Health Information Is Currently Handled Within the Employer		
1. Identify health plans subject to HIPAA and individuals with access to health information— • identify health plans subject to HIPAA • identify internal personnel with access to health information • describe known uses for health information • list outside entities/vendors with which health information is shared • list outside entities/vendors that provide health information		
2. Identify non-health plans and programs with access to health information— • identify non-health plans/programs subject to HIPAA • identify internal personnel with access to health information • describe known uses for health information • list outside entities/vendors with which health information is shared • list outside entities/vendors that provide health information		
3. Identify additional individuals with access to health information e-mail/intranet survey.		
4. Identify specific health information exchanges engaged in by personnel identified in Steps 1-3— • identify specific health information uses and disclosures • identify purpose for which health information is currently used and disclosed • identify source of health information • identify outside entities with which health information is shared (and purpose of sharing information) • determine whether release/authorizations are currently used • determine privacy policies, procedures and safeguards currently in place		
Evaluate the Employer's Need for Protected Health Information and Desired Approach ("Hands Off" or "Involved")		
In complying with the HIPAA privacy rules, the regulations allow plan sponsor to choose between the "Hands-Off PHI" Approach and the "Hands-On" Approach • "Hands-Off PHI" Approach: Group health plans that provide health benefits only through an insurance contract (fully-insured plans), and that do n*ot* create, maintain, or receive PHI, can largely avoid the burdensome privacy requirements • "Hands-On" Approach: Group health plans that either are self-insured or are fully insured and create, maintain, or receive PHI (in addition to summary health information and enrollment information) are subject to all of HIPAA privacy requirements		

Task	Tasks Assigned to	Status/Work Performed
Based on information obtained from the inquiries outlined above, the Employer must decide, with regard to *each* of its plans, whether it will adopt the "Hands-On" Approach or the "Hands-Off" PHI Approach.		
In choosing between the "Hands-Off PHI" Approach and the "Hands-On" Approach, the Employer must evaluate the benefits it offers, as well as its current level of involvement in administering health plans.		
1. List the various benefits offered (i.e., medical, dental, health FSA, EAP, vision, etc.).		
2. Identify whether each of the benefits is fully insured or self-insured.		
3. Identify the type of PHI that is involved with each benefit.		
4. Identify the purposes for which the PHI is currently being used within the Employer. These purposes should then be divided into three categories: • uses permitted by the privacy rules without an authorization • non-permitted uses that are deemed vital, and for which an employee authorization should thus be obtained • non-permitted uses that are not vital and should thus be discontinued		
5. Evaluate whether other uses are necessary and permitted. • determine whether such uses are permissible under the privacy rules • if not, evaluate whether the uses are vital enough to seek an employee authorization so that the uses are permitted under the rules		
6. Determine whether any safeguards are already in place to protect the PHI. • compare these safeguards to those that are required by HIPAA (discussed below) determine what changes will need to be made		
7. For fully-insured benefits, determine the extent to which the Employer desires to have PHI access that extends beyond the following t two scenarios: • obtaining from the group health plan or its health insurance issuer (upon request) "summary health information" for the limited purposes of (a) obtaining premium bids for providing health insurance coverage under the group health plan; or (b) modifying, amending or terminating the group health plan • obtaining information relating to enrollment and disenrollment under the group health plan. The Employer can choose the "Hands-Off PHI" approach if it is willing to limit its access to PHI these two scenarios.		
"Hands-On" Approach		
Health plans are subject to the following HIPAA administrative requirements if the Employer adopts the "Hands-On" approach. Health plans (acting through the privacy officer) should ensure that compliance with the HIPAA's privacy rule is well documented.		
1. Administrative requirements • appoint a privacy officer; • establish policies and procedures for the use and disclosure of PHI; • establish a complaint office; • train employees regarding privacy rules; • adopt a sanctions policy for employees that violate the HIPAA privacy rule; • adopt procedures prohibiting retaliation against individuals who exercise HIPAA rights and to avoid a waiver of those rights; and • establish physical, technical and administrative safeguards to protect PHI		
2. Prepare and distribute a Notice of Privacy Practices • a description of uses and disclosures of PHI, • right to inspect and obtain a copy of PHI; • right to have the Plan amend PHI records; • right to request restrictions on certain disclosures of PHI and to request confidential communications of PHI; and • right to receive an accounting of disclosures of PHI made within past six years		
3. Design and implement internal procedures to permit individuals to exercise their HIPAA rights • provide notice of privacy practices; • provide notice of right to inspect and obtain a copy of PHI, request amendment of PHI, request restrictions on certain uses and disclosures of PHI, request and		

Task	Tasks Assigned to	Status/Work Performed
received(if the request is reasonable) confidential communications of PHI by alternative means or at alternative locations and obtain an accounting of disclosures of PHI; and • explain where and how individual can file a HIPAA privacy complaint		
It is important to remember that even after complying with these administrative requirements, the Employer can use PHI *only for limited purposes*— namely, for "plan administration functions" that are performed on behalf of the group health plan and that are specified in the plan document. Moreover, only the "minimum necessary" PHI can be disclosed to accomplish the function. Moreover, the privacy officer should ensure that the policies and procedures (and related documents) are reviewed and updated periodically to reflect changes in circumstances (including operational changes, structural changes, and personnel changes).		
Amend the Plan Document		
In order for a plan to disclose PHI to the Employer's benefits personnel, the plan document must be amended to: • describe the permitted and required uses and disclosures of PHI by the plan; • specify that disclosure is permitted only upon receipt of written certification that the plan documents have been amended; and • provide adequate firewalls Each of these is discussed in more detail below.		
1. Describe the permitted and required uses and disclosures. The plan document must be amended to establish the permitted and required uses and disclosures of PHI. This must be addressed in the plan's Notice of Privacy Practices.		
2. Include written certification that plan documents have been amended. The plan document must be amended to provide that the plan may disclose PHI to the Employer *only* if the Employer certifies that the plan documents have been amended to incorporate the following provisions and that the Employer agrees to: • not use or further disclose PHI other than as permitted by the plan documents or as required by law; • ensure that any agents or subcontractors to whom it provides PHI received from the health plan agree to and comply with the same restrictions and conditions that apply to the Employer; • not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan; • report to the health plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures; • make PHI available to plan participants, consider their amendments, and, upon request, provide them with an accounting of PHI disclosures; • make its internal practices and records relating to the use and disclosure of PHI received from the health plan available to HHS upon request; and • if feasible, return or destroy all PHI received from the health plan that the Employer maintains in any form and retain no copies of such information when no longer needed for the purpose for which 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).		
3. Erect firewalls. In order to ensure that "adequate separation" exists between the group health plan and the Employer, the plan must be amended to: • describe the employees (or class of employees) who may be given access to PHI; • restrict access to and use by such employees to *plan administration functions* that the Employer performs for the health plan; and • provide a procedure for resolving any issues of non-compliance		
Erect Firewalls		
Covered entities are required to erect "firewalls" to prevent PHI from being used impermissibly.		

Task	Tasks Assigned to	Status/Work Performed
1. Evaluate the roles of all employees to determine which employees are involved in the administration of its benefit plans.		
2. Implement a procedure to ensure that only these designated employees have access to PHI, and even then, that they have access only to the PHI necessary to perform their duties for the plan.		
3. Implement a mechanism for ensuring that these employees do not use or disclose PHI in a way prohibited by the privacy regulations. • provide educational training for employees concerning the HIPAA privacy rules, the statutory penalties associated with violation of the rules, and the Employer's internal policies for dealing with such violations		
Develop Approach to Comply with Breach Notification Requirements		
An action plan is required to ensure compliance with notification requirements in instances where there is a breach of unsecured PHI.		
1. Establish processes for identifying and responding to breaches including mitigation of "compromises" the security or privacy of PHI.		
2. Establish breach notification procedures (to individuals, HHS, and in certain instances, to the media).		
3. Amend business associate contracts.		
4. Undertake workforce training.		
5. Comply with additional administrative requirements (e.g., revisions to policies and procedures, complaint process).		
Address Relationships With Outside Third Parties (Vendors, TPAs, etc.)		
The privacy regulations require that certain restrictions be placed on health information that flows from the Employer to third parties known as "business associates."		
1, Identify which third parties constitute "business associates." HIPAA provides that a "business associate" is a person who, on behalf of a covered entity (i.e., a health care provider, health plan, or health care clearinghouse)— • performs or assists in performing a function or activity involving the use or disclosure of individually identifiable health information or involving any other function or activity regulated by HIPAA's administrative simplification rules; or • provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, health information services, e-prescribing gateways, data transmission services, and subcontractors, of a covered entity. where the performance of such services involves providing such service provider with individually identifiable health information.		
2. Ensure that each business associate contract: • describes the permitted and required uses and disclosures by the business associate, which may not exceed that which is allowed for the plan; • prohibits the business associate from disclosing the information further; • requires the business associate to implement safeguards to prevent the improper use and disclosure of information; • requires the business associate to report to the plan any improper use or disclosure of PHI; • imposes the same requirements on all of the business associate's subcontractors; • requires the business associate to make available PHI in compliance with individuals' rights to access, amend, and receive an accounting related to such PHI; • requires the business associate to make its internal books and records available to HHS for purposes of determining the covered entity's compliance with HIPAA; • describes the steps the business associate is required to take with respect to breach notification requirements and mitigation of breaches; • requires the business associate to return or destroy PHI, if feasible, upon termination of the relationship; and authorizes the plan to terminate the contract if the business associate has violated a material term of the contract; • authorizes the plan to terminate the contract if the business associate has		

Task	Tasks Assigned to	Status/Work Performed
violated a material term of the contract		
3. Consider contractual provisions to address breaches of breaches the contract. The provisions could include a unilateral right to terminate the contract upon a material breach of HIPAA obligations, as well as indemnity to the plan (and the Employer) for any damages that the plan (or the Company) may incur by reason of the business associate's breach		
4. Ensure that *all* business associates properly sign the contract and educate the business associates regarding their responsibilities and obligations under the contract.		
5. Implement a program to address the plan's obligations in the event a business associate breaches the contract. • if the plan obtains knowledge of a pattern or practice by a business associate that violates the business associate contract, the plan is required to take reasonable steps to cure the breach or end the violation • if the reasonable steps are unsuccessful, the plan must terminate the business associate contract, or (if not feasible) report the business associate to HHS		
Evaluate Potential Impact of Privacy Regulations on Non-Health-Plan Operations		
Although the HIPAA privacy regulations are targeted at health plans, they will have some impact on non-health-plan operations (workers' compensation, disability, work return, etc.) that rely on access to individual health information. It is therefore important that the Employer consider how its non health-plan operations may be affected by the privacy rules. Some areas to consider are set forth below. The Employer should evaluate all of its non-health plan operations to see if there are additional areas.		
Formalize Privacy Policy to Reflect Approach Taken and Specific Organizational Requirements		
1. *Drug testing policies.* Medical providers generally will not perform drug tests without authorization by the employee. The regulations do not prohibit a plan from requiring an employee to provide such authorization as a prerequisite to his or her employment (but other federal laws, such as ADA, should be reviewed).		
2. *Disability, FMLA, life insurance underwriting and administration.* An employee's authorization generally is required before the Employer can use PHI for non-health-plan purposes such as disability, FMLA, life insurance underwriting, etc.		
3. Other Current Uses of PHI		