Employer-Sponsored Health Plan HIPAA Compliance Checklist

The administrative simplification provision of the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA) impose obligations on employer-sponsored group health plans. Given recent high-profile HIPAA enforcement actions, employers should understand their compliance obligations. This checklist is intended to assist plan sponsors with HIPAA compliance for their plans.

HIPAA covers "group health plans," which are both insured and self-insured employee welfare benefit plans that (i) have 50 or more participants or use a third party administrator and (ii) provide health benefits. Depending on the nature of the group health plan, an employer, in its role as the plan sponsor or administrator, may need to comply with HIPAA and safeguard protected health information (PHI).

1. IMMEDIATE GROUP HEALTH PLAN ACTION ITEMS:

- ☐ Determine if and which plans are subject to HIPAA. This may include health, dental, and vision benefits, employee assistance programs, health reimbursement arrangements, and health spending accounts.
- ☐ Appoint a privacy official, security official, and contact person (which can be the same person) and outline their respective roles and responsibilities.
- ☐ Identify where, why, and to what extent PHI is created, received, maintained, or transmitted by the plans and involve IT, payroll, HR, legal, and other departments that may handle PHI.
- ☐ Verify how the plans use or disclose PHI and analyze permissibility under HIPAA.
- ☐ Determine whether authorizations can be obtained for otherwise impermissible uses and disclosures.
- ☐ Verify that plan documents are HIPAA-compliant, including meeting the privacy and security requirements for plan documents.
- ☐ For plans with "hands-on" access to PHI, verify that plan documents grant access to plan PHI to all appropriate employees of the plan sponsor, which could include HR, IT, finance, payroll, and legal, for example.
- ☐ Verify that HIPAA-compliant certification is in place to the extent that the plan sponsor is handling PHI for plan administration.
- ☐ Determine which other federal and state privacy and security laws apply to the plans and verify compliance.

2. ESTABLISH AND MAINTAIN PRIVACY STANDARDS FOR HEALTH PLANS

- ☐ **Self-insured health plan**
  - Develop HIPAA-compliant privacy policies establishing permitted and required uses and disclosures of PHI.
  - Establish policies, procedures, and processes to comply with individual rights with respect to PHI.
  - Implement administrative requirements, such as a training program and sanctions policy for noncompliance with HIPAA.
  - Allocate relevant responsibilities between and among plans, plan sponsors, and third-party service providers, including development and distribution of the notice of privacy practices.

- ☐ **Fully insured health plan where plan sponsor does not have access to PHI**
  - Verify that PHI, except for enrollment/disenrollment or summary health information, is not shared with plan sponsor.
  - Establish policies prohibiting retaliation and waiver of rights.
  - Consider developing a privacy policy.
  - Verify that the insurer is complying with HIPAA privacy requirements (e.g., maintaining privacy policies, complying with individual rights to PHI, providing the notice of privacy practices, etc.).

- ☐ **Fully insured health plan where plan sponsor has access to PHI through the plan**
  - Allocate relevant responsibilities between and among plans, plan sponsors, and third-party service providers, including a process to address compliance with individual rights with respect to PHI.

3. ESTABLISH AND MAINTAIN SECURITY STANDARDS FOR HEALTH PLANS

- ☐ Conduct, develop, and document a risk analysis that meets HIPAA requirements.
- ☐ Develop a risk management plan based on the risk analysis.
- ☐ Revisit and update risk analysis and risk management plan regularly and in response to organizational changes, external threats, security incidents, and data breaches.
- ☐ Develop HIPAA compliant security policies and procedures that establish security responsibilities or delegate those responsibilities to the relevant sponsor, third-party service provider, or business associate.

4. ESTABLISH AND MAINTAIN BREACH NOTIFICATION STANDARDS FOR HEALTH PLANS

- ☐ Develop HIPAA-compliant breach policies that establish breach response procedures, timely notification requirements, and appropriate notification standards.
- ☐ Coordinate breach notification responsibilities with business associates and third-party service providers.
- ☐ Identify outside resources that can assist a plan in the event of a potential breach, including outside legal counsel, forensic consultants, identity theft protection, and breach response vendors.
- ☐ Obtain or revisit cyberinsurance coverage.

5. ADDRESS BUSINESS ASSOCIATE REQUIREMENTS

- ☐ Identify business associates of plans. These are third parties that provide services to the plans that involve the creation, receipt, maintenance, or transmission of PHI (such as most third party administrators).
- ☐ Verify that business associate contracts are in place with each business associate.
- ☐ Verify that all business associate contracts comply with HIPAA privacy and security requirements.
- ☐ Track all business associate agreements (e.g. contracts with third-party administrators, consulting firms, legal service providers, accountants, etc.).

6. EMPLOYEE TRAINING

- ☐ Provide employee training so workforce members are familiar with HIPAA's privacy, security, and breach response notification standards and the plan policies, procedures, and processes.

7. ESTABLISH AND MAINTAIN A CULTURE OF COMPLIANCE

- ☐ Emphasize the importance of privacy and security.

Use of this checklist is not intended as a guarantee that you are or will be fully HIPAA compliant. Contact your DWT attorney for information on HIPAA training and customizing required policies and procedures.

Dipa N. Sudra | Partner | Seattle | 206.757.8270 | dipasudra@dwt.com

Rebecca L. Williams | Partner | Seattle | 206.757.8171 | beckywilliams@dwt.com

Adam H. Greene | Partner | Washington, D.C. | 202.973.4213 | adamgreene@dwt.com

Sean R. Baird | Associate | Seattle | 206.757.8091 | seanbaird@dwt.com