Employer-Sponsored Health Plan HIPAA Compliance Checklist

The Administrative Simplification Section of the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA) impose compliance obligations on employer-sponsored group health plans. Given high-profile HIPAA enforcement actions, employers should understand these obligations. The following checklist is intended to assist plan sponsors with HIPAA privacy, security, and breach notification 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 undertake actions both directly and on behalf of its group health plan 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. These may include health, dental, and vision benefits, employee assistance programs, health reimbursement arrangements, and health spending accounts
- ☐ Determine whether any "organizational" arrangements apply and would be beneficial, such as "hybridizing" a wrap plan so only the health care component would be subject to HIPAA, designating an affiliated covered entity (ACE), or recognizing an organized health care arrangement (OHCA)
- ☐ Appoint a privacy official, security official, and contact person (which can be the same person) and document their respective roles and responsibilities
- ☐ Identify where, why, and to what extent PHI is created, received, maintained, or transmitted by the plan
- ☐ Verify that plan documents are HIPAA-compliant, including meeting the privacy and security requirements
- ☐ For self-insured plans and insured plans with "hands-on" access to PHI, verify plan documents grant access to PHI to all appropriate employees of the plan sponsor, who could include, for example, HR, IT, finance, payroll, and legal
- ☐ Verify that a HIPAA-compliant certification is in place to the extent the plan sponsor is handling PHI for plan administration
- ☐ Verify how the plan uses or discloses PHI and analyze permissibility under HIPAA, which may include obtaining authorizations
- ☐ 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 and procedures establishing permitted and required uses and disclosures of PHI and minimum necessary considerations
- Establish policies, procedures, and processes to comply with individual rights with respect to PHI (e.g., access, amendment, accounting of disclosures)
- Implement administrative requirements, such as sanctions/disciplinary policy for noncompliance with HIPAA and a training program
- Develop and appropriately provide notice of privacy practices
- Allocate relevant responsibilities between and among plans, plan sponsors, and third-party service providers

☐ **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 the requirements that apply to self-funded plans

☐ **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 and procedures prohibiting retaliation and waiver of rights
- Consider developing an abbreviated HIPAA 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)

3. ESTABLISH AND MAINTAIN SECURITY STANDARDS FOR HEALTH PLANS

☐ Conduct and document a security risk analysis to identify risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI that meets HIPAA requirements

☐ Develop a risk management plan that correlates with 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, procedures, and processes to protect the confidentiality, integrity, and availability of electronic PHI

☐ Verify that appropriate administrative, technical, and physical safeguards are in place

☐ 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 response and notification 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

☐ Develop an incident response plan and consider “table top” exercises

5. ADDRESS BUSINESS ASSOCIATE REQUIREMENTS

- ☐ Identify business associates of the plan. These are third parties that create, receive, maintain, or transmit PHI in providing services to the plan (such as most third-party administrators)
- ☐ Verify that a business associate agreement (BAA) is in place with each business associate
- ☐ Verify that all BAAs comply with HIPAA privacy and security requirements
- ☐ Maintain a list of all business associates and copies of all BAAs

6. WORKFORCE TRAINING

- ☐ Provide training to authorized workforce members, and possibly others, on the plan's privacy, security, and breach response and notification policies, procedures, and process
- ☐ 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, customizing required policies and procedures, and questions about HIPAA compliance.**

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

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

Allison De Tal
ASSOCIATE
206.757.8060 | Seattle
allisondetal@dwt.com

Adam Greene
PARTNER
202.973.4213 | Seattle
adamgreene@dwt.com