BALDWIN REGUALTORY COMPLIANCE COLLABORATIVE

HIPAA Security Rule Administrative Simplification Requirements

Checklist of Selected Administrative Requirements for Covered Entities, Business Associates and Related Sub-contractors

HIPAA rules detail the administrative requirements imposed upon all HIPAA covered entities, including covered private self-funded health and welfare benefit plans, as detailed below:

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
1.	**Does the covered entity have a Privacy Officer in accordance with 45 C.F.R. § 164.530(a)?**	A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.			
2.	**Does the covered entity have a Security Officer in accordance with 45 C.F.R. § 164.308(a)(2)?**	A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.			

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
3.	**Does the covered entity have written policies and procedures in place in accordance with 45 C.F.R. § 164.530(i)?**	A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule, and which govern the use of protected health information arising in connection with administration of the covered entity.			
4.	**Does the covered entity conduct workforce training and management in accordance with 45 C.F.R. §§160.103 and 164.530(b)?**	A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (regardless of whether they are paid by the entity).			
5.	**Does the covered entity have and apply an appropriate sanctions policy in accordance with 45 C.F.R. § 164.530(e)?**	A covered entity must have and apply appropriate sanctions against workforce members who violate the covered entity's privacy policies and procedures or the requirements of the Privacy Rule.			
6.	**Does the covered entity have and apply an appropriate harm mitigation policy in accordance with 45 C.F.R. § 164.530(f)?**	A covered entity must mitigate, to the extent practicable, any harmful effects it learns were caused by the improper or unlawful use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.			
7.	**Does the covered entity maintain reasonable and appropriate administrative, technical,**	A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in			

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
	and physical safeguards in accordance with 45 C.F.R. § 164.530(c)?	violation of the Privacy Rule. These safeguards also serve to limit any incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or passcode, and limiting access to keys or pass codes.			
8.	**Does the covered entity have and apply procedures for individuals to complain about its compliance with its privacy policies and procedures under the Privacy Rule in accordance with 45 C.F.R. §§ 164.530(d) and 164.520(b)(1)(vi)?**	A covered entity must have written procedures designed to apprise individuals of their right to complain about the entity's compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain such procedures in its Notice of Privacy Practices. Among other things, the covered entity must identify to whom individuals can submit complaints at the covered entity, as well as notice and contact information necessary to advise the Secretary of HHS of such complaints.			
9.	**Does (or has) the covered entity retaliate(d) against a person for exercising rights provided in the Privacy Rule, for assisting in an investigation, or for opposing an act or practice in violation of 45 C.F.R. § 164.530(g)?**	A covered entity may not retaliate against a person for exercising any right(s) guaranteed under the Privacy Rule, for assisting in inquiries and investigation by HHS or another appropriate authority, or for opposing any act or practice that the person believes in good faith violates the Privacy Rule. Further, a covered entity may not require any individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, enrollment or benefits eligibility.			

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
10.	**Does the covered entity maintain required documentation in accordance with 45 C.F.R. § 164.530(j)?**	A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.			
11.	**Does the covered entity provide a notice of its privacy practices (Privacy Notice) in accordance with 45 C.F.R. §§ 164.520(a) and (b)?**	Each covered entity, with certain exceptions, must provide a notice of its privacy practices (Privacy Notice). The Privacy Rule requires that the Privacy Notice contain certain elements. The Privacy Notice must: ▪ Describe the ways in which the covered entity may use and disclose protected health information. ▪ State the covered entity's duties to protect privacy, provide a Privacy Notice , and abide by the terms of the current Notice. ▪ Describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. ▪ Include a point of contact for further information and for making complaints to the covered entity. A covered entity must act in accordance with the Privacy Notice The Privacy Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.			

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
12.	**Does the covered entity have a business associate agreement or contract with each contractor or other non-workforce member that performs services or activities in accordance with 45 C.F.R. §§ 160.103, 164.502(e) and 164.504(e)?**	When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Privacy Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances, governmental entities may use alternative means to achieve the same protections). In the business associate agreement, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates. Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Privacy Rule.			
13.	**Has the covered entity performed a risk analysis(es) as part of the security management process in accordance with 45 C.F.R. §§ 164.306(b), *et sec.* and 64.308(a)(1)(ii), *et sec.*?**	The Administrative Safeguards provisions in the Security Rule require covered entities to perform a risk analysis as part of their security management processes. By helping to determine which security measures are reasonable and appropriate for a particular covered entity, a risk analysis affects the implementation of all the safeguards contained in the Security Rule. A risk analysis process includes, but is not limited to, the following activities: ▪ Evaluate the likelihood and impact of potential risks to e-PHI; ▪ Implement appropriate security measures to address the risks identified in the risk analysis;			

No.	Title of the Required Activity	Description of the Regulatory Required Activity	Responsible Party & Compliance Date	Standard Satisfied [YES / NO]	Notes and Observations
		▪ Document the chosen security measures and, where required, the rationale for adopting those measures; and ▪ Maintain continuous, reasonable, and appropriate security protections. Performing a risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI.			

For assistance with these and other requirements and obligations required by HIPAA's Security and Privacy Rules, please reach out to your local service advisor. Baldwin Risk Partners maintains several resources for self-funded plan sponsors that are covered entities under HIPAA, including Security Incident Procedures overview, training resources for all of HIPPA four main rules (Privacy, Security, Breach Notification, and Enforcement), as well as breach reporting templates and samples and related worksheets.