

Data Security and Breach Notification Checklist

STEP	DESCRIPTION	Done
1. Business Associate Review	<ul style="list-style-type: none"> a. Contact existing BA's and verify readiness to comply with HIPAA standards. b. Update BA agreement to include new privacy and security expectations for BA's. c. Execute updated BA agreements with all relevant parties. 	
2. Breach Notification	<ul style="list-style-type: none"> a. Create plan to address breach notification under HIPAA and verify satisfaction of state law standards. b. Update HIPAA policies and procedures to manage breach events. c. Create breach notification template letter. d. Train staff on new procedures. 	
3. PHI Restrictions	<ul style="list-style-type: none"> a. Revise policies and procedures to support PHI disclosure restriction requests. ("I don't want the following information released.") b. Ensure data systems can identify data affected by these requests. c. Train staff to identify and comply with such requests. 	
4. Electronic Health Records Request	<ul style="list-style-type: none"> a. Revise policies and procedures to support requests to obtain a copy of information contained in an individual's HER b. Train staff to comply with such requests. 	
5. Marketing Activities	<ul style="list-style-type: none"> a. Amend policies and procedures to address updated HIPAA marketing guidelines. (New restrictions on 3rd party use and access.) b. Train staff on restrictions. 	
6. "Minimum Necessary" Standards	<ul style="list-style-type: none"> a. Revise and execute new "minimum necessary" policies in accordance with HHS guidance. b. Train staff on limiting disclosures. 	
7. Accounting for Disclosures	<ul style="list-style-type: none"> a. Revise policies and procedures to address individual requests for an accounting of PHI disclosures. b. Ensure systems can track disclosures, including remote access if any. 	
8. Privacy Policy	<p>Update privacy policies to include:</p> <ul style="list-style-type: none"> • Breach notification • PHI restrictions Electronic record requests • Marketing changes • "Minimum necessary" guideline compliance • Post updated policy as required and share with all BA's 	
9. Verify Provider Contract Compliance	<p>Review existing provider agreements to ensure compliance with any and all terms and conditions governing data management, medical record maintenance, and HIPAA/HITECH.</p> <p>Review provider agreements to ensure compliance with billing procedures including requirements for electronic transactions.</p>	