

Questions	Y	N	Action
6. Have any prior Risk Assessments, security tests, or audits been done for your agency?	<input type="checkbox"/>	<input type="checkbox"/>	If Yes, please list the date(s) the assessment was done. _____ _____
7. If Risk Assessments have been conducted, please state why they were done.			_____ _____ _____ _____
8. Does your agency create PHR (personal health records)?	<input type="checkbox"/>	<input type="checkbox"/>	If Yes, what steps have been taken to ensure security and privacy of these records? _____ _____ _____ _____

HIPAA-HITECH Definitions

As Needed: Identifies the reasons why Risk Assessments are conducted; to reflect a change in a contract, changes in programs or personnel, requirements of a grant, new or updated software, or similar significant changes.

Breach: The acquisition, access, use or disclosure of Protected Health Information in a manner **not permitted by HIPAA or the HITECH Act and associated regulations, which compromises the** security or privacy of such information or records. Compromising the security or privacy of such information or records means that the acquisition, access, use or disclosure poses a significant risk of financial, reputational, or other harm to the individual.

Business Associate: A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce, and that has access to PHI. A business associate may also be a covered entity in its own right.

Electronic Protected Health Information (ePHI): Individually identifiable health information that is transmitted by electronic media or maintained in electronic media. Exclusions include education records covered by the Family Educational Rights and Privacy Act (20 USC 1232g, which excludes certain treatment records described in section 1232g(a)(4)(B)(iv)) and employment records held by a covered entity in its role as an employer.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and its implementing regulations, including 45 CFR 160 and 164.

HITECH Act: The American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act, Public Law 111-005.

PHR: A Personal Health Record that contains electronic individual identifiable health information (created or received from health care provider, health plan, employer, or health care clearinghouse that relates to past, present or future health; the provision of health care; or payment for health care and identifies the individual) and has to be provided for or on behalf of the individual (like a benefit) and that identifies or can identify the individual.

Questions	Y	N	Action
-----------	---	---	--------

Risk analysis: The assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (e-PHI) held by a covered entity, and the likelihood of occurrence.

Risk management: The actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its e-PHI and to meet the general security standards.