Policies and Procedures Audit Checklist for HIPAA Privacy, Security, and Breach Notification

Type of Policy and Procedure	Comments	Completed
Policy to Maintain and Update Notice of Privacy Practices		
Notice of Privacy Practices	Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of privacy practices and an individual's privacy rights. Develop policies and procedures.	
Uses and disclosures consistent with Notice of Privacy Practices	Uses and disclosures of PHI must be in a manner that is consistent with Notice of Privacy Practices. Uses and disclosures must be outlined in Notice of Privacy Practices. Develop policies and procedures.	
Policy for Documentation of Compliance Activity		
Document retention	Policy and procedures for document retention should last a minimum of six years. Develop policies and procedures.	
Policy for Limitation on Access		
Workforce member training	A covered entity is required to train all members of its workforce on the policies and procedures related to PHI under HIPAA, as necessary and appropriate according to the function of each member's position within the workforce. Develop policies, procedures, forms, and training.	
Minimum Necessary Uses and Disclosures of PHI	The Plan and the organization shall take reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when using or disclosing PHI or seeking PHI from another covered entity. Develop policies and procedures.	
Use and disclosure of PHI by plan sponsor	Develop policies and procedures.	

Type of Policy and Procedure	Comments	Completed
Policies for Handling Individual Rights		
Confidential communications	Individuals may request to receive PHI communications by alternative means or at alternative locations. Develop policies, procedures, and forms.	
Right of individual to request restriction on use or disclosure of PHI	Individuals have a right to request restrictions on uses and disclosures of PHI about the individual to carry out treatment, payment and health care operations, and disclosures made to family members or persons who are involved in the health care of the individual. Develop policies, procedures, and forms.	
Right of individual to access or amend own PHI	Individuals have the right to review or obtain copies of their own PHI. Individuals also have the right to request amendments to their PHI, with some exception. Develop policies, procedures, and forms.	
Termination of restriction on use or disclosure of PHI	Develop policies, procedures, and forms.	
Right of individual to amend PHI	Individuals have the right to amend or correct their PHI. Develop policies, procedures, and forms.	
Right to request an accounting of disclosures	Individuals have the right to request an accounting of disclosures that are beyond certain parameters. Develop policies, procedures, and forms.	
Policies and Procedures for Using and Disclosing PHI		
Uses and disclosures of PHI when individual is present	If the individual is present, the covered entity may use or disclose PHI if the covered entity obtains the individual's consent, provides an opportunity to object, or determines there is no objection based on circumstances (e.g., with a translator). Develop policies and procedures.	
Limitations on uses and disclosure of PHI when individual not present	If the individual is not present, the covered entity may determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's healthcare or needed for notification purposes (e.g., individual is incapacitated). Develop policies and procedures.	

Type of Policy and Procedure	Comments	Completed
Determination as to whether authorization is valid	Develop policies and procedures.	
Verification of individuals who request PHI	Develop policies and procedures for the verification of the identity of those requesting PHI. Include policies and procedures for: individual, spouse, domestic partner, civil union partner, parent seeking the PHI of a minor child, authorized personal representative, public officials, and person involved in individuals' care. Develop policies and procedures.	
Uses and disclosures of PHI to family members, relatives, close personal friends, or others authorized by individual (Personal Representatives)	Develop policies and procedures.	
Terminating a restriction on the use or disclosure of PHI	Develop policies and procedures.	
Uses and disclosures for underwriting and related purposes	A plan that performs underwriting (including but not limited to setting a plan's premium, employee contributions or granting a premium reduction to an individual) may not use or disclose PHI that is genetic information for underwriting purposes, except in the case of long term care coverage. Develop policies and procedures.	
Limited data sets and data use agreements	Ensure that data use agreements cover the use and disclosure of limited data sets. Although still PHI, a covered entity may use and disclose limited data sets. Develop policies and procedures.	
Re-identification of PHI	Develop policies and procedures.	
De-identification of PHI	De-identified Information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Policies and procedures for de-identifying PHI should include an explanation of identifiers. Develop policies and procedures.	
Permitted uses and disclosures	Outline permitted uses and disclosures of PHI. Develop policies and procedures.	

Type of Policy and Procedure	Comments	Completed
Uses and disclosures pursuant to an authorization	Outline permitted uses and disclosures of PHI allowed pursuant to an authorization. Develop policies, procedures, and forms.	
Deceased individuals	Plan may disclose PHI of a deceased person to family or other individuals involved in the person's care prior to their death unless doing so is "inconsistent with any prior expressed preference" of the deceased, if known. Develop policies and procedures.	
Personal Representatives	Personal Representative may request PHI on individual's behalf. Individual must designate Personal Representative using "Designation of Personal Representative." Policy and procedure should exist for verification of the identity of the Personal Representative requesting the PHI. Develop policies, procedures, and forms.	
Policies and Procedures for Disclosure for Legal or Public Policy Reasons		
Whistleblowers	Whistleblowers are protected when disclosing PHI to oversight authorities. Develop policies and procedures.	
Disclosures by workforce members who are victims of a crime	Disclosure of PHI in certain cases for victims of a crime. Develop policies and procedures.	
Uses and disclosures of PHI for judicial and administrative proceedings	A health plan may disclose PHI for judicial and administrative proceedings with notice to the individual. Develop policies and procedures.	
Uses and disclosures of PHI when required by law	Develop policies and procedures.	
Uses and disclosures of PHI for public health activities	Develop policies and procedures.	
Disclosures of PHI about victims of abuse, neglect, or domestic violence	Develop policies and procedures.	
Disclosures for health oversight activities	Develop policies and procedures.	
Disclosures for law enforcement purposes	Develop policies and procedures.	

Type of Policy and Procedure	Comments	Completed
Uses and disclosures for cadaveric organ, eye or tissue	Develop policies and procedures.	
Disclosures for Armed Forces activities	Develop policies and procedures.	
Disclosures for prisoners	Develop policies and procedures.	
Disclosures for workers' compensation purposes	Develop policies and procedures.	
Miscellaneous Policies and Procedures		
Prohibition on conditioning treatment, payment, or healthcare operations on provision of authorization	Develop policies and procedures.	
Opportunity to object to use or disclosure	Develop policies, procedures, and forms.	
Business Associate contracts	Develop policies, procedures, and model agreements outlining the handling and use of PHI by Business Associate.	
Handling complaints	Complaints should be sent to, investigated, and tracked by the Privacy Officer. Develop policies, procedures, and forms.	
Sanctions for violations	Must have sanctions against workforce members that violate privacy policies and procedures. Develop policies, procedures, and forms.	
Mitigation of harm	Must, to extent practicable, mitigate any known harmful effect of a use or disclosure of PHI in violation of its own policies and procedures or of HIPAA regulations by its own workforce members or a business associate. Develop policies and procedures.	
Refraining from intimidating or retaliatory acts	May not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against an individual who exercises a HIPAA right or participates in the filing of a complaint either under the covered entity's own policies and procedures or with HHS. Develop policies and procedures. Include in training.	

Type of Policy and Procedure	Comments	Completed
Administrative, Technical, and Physical Safeguards		
Reasonable safeguards to protect PHI from unintentional use or disclosure (Privacy)	Must have reasonable safeguards to protect PHI from unintentional use or disclosure of PHI. Develop policies and procedures.	
Conducting periodic risk assessments (Security)	Must have policies and procedures to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Develop policies and procedures. Document measures.	
Acquisition of IT Systems (Security)	Must have processes in place for the selection of IT systems and services. Develop policies and procedures. Document measures.	
Information System Activity (Security)	Must have policies and procedures for regulating viewing of information system activity. Develop policies and procedures. Document measures.	
Risk Management program (Security)	Must have property security measures in place to reduce the risk of security threats. Develop policies and procedures. Document measures.	
Authorization and/or supervision of workforce members (Security) (Addressable)	Develop policies, procedures, and forms for documentation. Document measures.	
Appropriate level of access (Security) (Addressable)	Must implement policies and procedures to ensure appropriate access to ePHI by establishing clear job descriptions and responsibilities. Develop policies and procedures. Document measures.	
Appropriate criteria for access (Security) (Addressable)	Must implement policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks. Develop policies and procedures. Document measures.	
Establishment of workforce clearance (Security) (Addressable)	Must have process to determine whether a person should have access. Develop policies and procedures. Document measures.	
Breach Notification		
Risk assessment	Must have policies and procedures in place to determine whether a breach exists. Develop policies, procedures, and forms.	

Type of Policy and Procedure	Comments	Completed
Notification of Breach to individuals	Should have model forms for tracking, investigating, and providing notification of breach. Develop model forms.	
Timeliness of Notification of Breach	Should have process to provide timely notification. Develop policies and procedures.	
Notification of Breach methodology	Documents providing methods for notifying individuals will be compared to actual performance. Develop policies and procedures, including means to notify next of kin or personal representative and how to follow up if contact information is insufficient.	
Notification Content	Notices must have specific content. Develop standard templates or forms.	