HIPAA Audit Preparation Checklist

|  |  |
| --- | --- |
|  | Appoint a HIPAA Privacy Officer and Security Officer. (They may be the same person) |
|  | Appoint a contact person to handle complaints and respond to patient requests consistent with the NPP. |
|  | Define and document job description and roles and responsibilities for Privacy and Security Officials. |
|  | Inventory and document the location and security of PHI, whether hard copy, electronic, or spoken. |
|  | Document uses and disclosures permitted especially as it relates to treatment, payment and operations. |
|  | Determine staff and departments that have access to PHI, the level of access and whether the access is appropriate. |
|  | Identify and document procedures used for routine requests of PHI. |
|  | Ensure policies and procedures are in place related to uses and disclosures of PHI. |
|  | Ensure policies and procedures are in place related to disclosures that are consistent with the minimum necessary requirement. |
|  | Identify and document all business associates. |
|  | Ensure that a Business Associate Agreement or contract, consistent with the Omnibus rule have been executed with all business associates. |
|  | Ensure that policies and procedures are in place governing all HIPAA requirements including privacy, security and breach notification. |
|  | Ensure that workforce members who have access to PHI have received appropriate training on policies and procedures and relevant regulatory requirements. Document participation. |
|  | Use appropriate forms and checklists to ensure proper authorization for the disclosure of PHI. |
|  | Use appropriate forms and checklists to verify the status of personal representatives of individuals. |
|  | Distribute and post notice of privacy practices (NPP) to patients and individuals prior to first encounter with the patient. |
|  | Whenever possible, obtain acknowledgement of receipt of NPP from the patient or individual |
|  | Develop and implement reasonable administrative, technical and physical safeguards and policies and procedures ensuring the privacy and security of PHI. |
|  | Conduct a HIPAA security risk analysis documenting the threats and vulnerabilities to the confidentiality, integrity and availability of ePHI. |
|  | Document the risks to ePHI identified during the risk analysis and recommended remedial actions to lower the risk to a reasonable level. |
|  | Update your HIPAA security risk analysis periodically consistent with policy but at a minimum annually or when there is a significant change in the operating environment that might compromise the security of ePHI. |
|  | Conduct and encryption analysis and encrypt the transmission and storage of ePHI when reasonable and appropriate. |
|  | Develop, implement and document a contingency plan including requirements related to data backup, emergency response and disaster recovery. |
|  | Develop and implement procedures related to responding to and reporting privacy and security incidences. |
|  | Develop and implement procedures related to responding to breaches or potential breaches of PHI. |
|  | Ensure that HIPAA policies and procedures are consistent with Federal Law and comply with State law that are more restrictive than Federal Law. |
|  | Maintain HIPAA compliance documentation in written or electronic form for at least 6 years from the date the document was created or last in effect. |