CHECKLIST

HIPAA Security Checklist

The following are identified by HHS OCR as elements of an effective compliance program

Please check off as applicable to self-evaluate your practice or organization.

Have you conducted the following six (6) required annual Audits/Assessements?

- [ ] Security Risk Assessment
- [ ] Privacy Standards Audit (Not required for BAs)
- [ ] HITECH Subtitle D Audit
- [ ] Security Standards Audit
- [ ] Asset and Device Audit
- [ ] Physical Site Audit

Have you implemented a security awareness and training program for all workforce members, including management?

- [ ] Are all workforce members trained about security reminders and security updates, on a periodic basis?
- [ ] Are all workforce members periodically trained about procedures for guarding against, detecting & reporting malicious software?
- [ ] Has your organization designated a Security Officer?

Has your organization developed a contingency plan for emergencies?

- [ ] Has your organization developed a disaster recovery plan for emergencies?
- [ ] Have you developed policies & procedures for responding to emergency situations?
- [ ] Do you regularly review and update your contingency plan and run test exercises?

Using a risk analysis, have you assessed whether data encryption is appropriate?

- [ ] If encryption is appropriate, have you developed encryption measures?
- [ ] Have you implemented controls to guard against unauthorized access of ePHI during electronic transmission?
- [ ] Have you assigned unique usernames / numbers to all individuals who require access to ePHI?

Are all permitted uses and disclosures of ePHI limited to the minimum necessary information to achieve the purpose for which ePHI is disclosed?

In addition to performing a risk analysis, does your organization have a sanction policy in place, in which appropriate sanctions are applied against workforce members that fail to comply with your security policies & procedures?

- [ ] Have you implemented controls to ensure ePHI cannot be altered or destroyed in an unauthorized manner?
- [ ] Have you developed policies & procedures that cover how to securely dispose of ePHI?
- [ ] Are electronic devices containing ePHI and physical PHI stored securely until they are disposed of in a secure fashion?

- [ ] In addition to conducting a risk analysis, have you implemented an information system activity review, by implementing procedures to regularly review records of information system activity such as:
  - Audit logs
  - Access reports
  - Security incident tracking reports

Do you have a defined process for incidents or breaches?

Need help completing your Checklist?

- [ ] (For covered entities) Do you obtain satisfactory assurances from business associates that they will appropriately safeguard ePHI that they create, maintain, receive, or transmit on your behalf?
- [ ] (For business associates) Do you permit subcontractors to create, receive, maintain, or transmit ePHI on your behalf only if you obtain satisfactory assurances that the subcontractor will appropriately safeguard the information?

- [ ] Speak to a backup expert about your environment today: https://www.novabackup.com/healthcare-backup-solutions

This checklist is composed of general questions about the measures your organization should have in place to state that you are HIPAA compliant and does not qualify as legal advice. Successfully completing this checklist does not certify that you or your organization are HIPAA compliance.

NovaBACKUP Corporation
29209 Canwood Street
Agoura Hills, California

Tel.: (805) 579-6700

Email: ols@novabackup.com
www.novabackup.com