GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

Office of Healthcare Privacy and Confidentiality

Last edited 11/2016

Business Associate HIPAA Compliance Questionnaire

The following questionnaire will help the District determine the whether Business Associates comply with regulations implementing both the Health Insurance Portability Accountability Act of 1996, as amended (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA). On an annual basis, by October 1, Business Associates are required to complete and return this questionnaire to the Agency Privacy Liaison or Agency Contract Administrator at the applicable District agency. At the District's discretion, this questionnaire may be required during the bidding process, or otherwise prior to the award of a contract.

Business Associate Profile:

Company Name:	
Contact Person:	
Phone:	
Email:	
Fax:	
Website:	
Addresses in USA where District government data would be shared:	
Address of Locations Outside USA:	

HIPAA Compliance Check list

Name of Business Associate's HIPAA Compliance Officer:	
Address:	
Phone:	
Email:	

Workforce Training

1. Is your HIPAA compliance officer certified in HIPAA Privacy/ Security?	
2. Provide years of experience.	
3. If not certified then which other comprehensive HIPAA training has been undertaken by HIPAA compliance officer. Provide course outline (Add separate sheet to answer this question):	
4. Provide date(s) of the training and length of training?	
5. Were the American Reinvestment and Recovery Act of 2009 and the Health Information Technology for Economic and clinical Health Act updates to HIPAA & the Omnibus Rule of 2013 included in the training?	
6. List details regarding any other employee(s) who has/have gone through comprehensive training, inclusive of who completed which training?	
7. Provide details of the course outline of employee training (Add separate sheet to answer this question).	
8. Provide percentage of employees and contractors who have completed required HIPAA training.	

General Security Safeguards

9. Have you conducted HIPAA Risk Analysis/Assessment for Security and Privacy?	
10. When was HIPAA Risk Analysis/Assessment conducted and by whom was it performed?	
11. Have you done vulnerability assessment of your network?	
12. Have you created HIPAA privacy policies? When were they updated? Provide list of all the Privacy policies. (Add separate sheet to answer this question)	

13. Have you created HIPAA security policies? When were they updated? Provide list of all the Security policies by title. (Add separate sheet to answer this question)	
14. Are employees trained & informed about your company's policies created for HIPAA?	
15. Are you required to create contingency plan? If yes, have you created contingency plan? When was it last tested (if answer is yes then respond to questions 16-21)	
16. Have you conducted application & data criticality analysis? (We may request to review your plan based on response to the questionnaire)	
17. Have you conducted facility risk assessment? (We may request to review your plan based on response to the questionnaire)	
18. Have you created data center disaster recovery plan? (We may request to review your plan based on response to the questionnaire)	
19. Have you created data backup plan? (We may request to review your plan based on response to the questionnaire)	
20. Have you created Emergency Mode of Operations Plan? (We may request to review your plan based on response to the questionnaire)	
21. Have you created testing and revision procedures? (We may request to review your plan based on response to the questionnaire)	
22. When was the last time you did audit to determine your HIPAA compliance status?	
23. Based on your knowledge, since what date	

were you HIPAA complaint?	

Access and Mobile Date Controls

24. Do you have documented data access policies and controls?	
25. Do you have a documented work from home policy and data access controls?	
26. Do you have mobile data policies and controls?	
27. Do you have "bring your own device" data polices and controls?	

Outsourcing

28. Do you outsource work to sub-contractors who may have access to our data and PHI?	
29. Are all your sub-contractors in USA? If not then please list in which countries are they located?	
30. Do you have business associate agreement with them to ensure HIPAA compliance of your subcontractors?	
31. Have your sub-contractors achieved HIPAA compliance?	
32. How do you verify sub-contractor compliance?	

Other Data Practices

33. Do you sell or rent data?	
34. Do you contract with subcontractors who sell or rent data?	

_____

Signature of Contractor Principal

Printed Name:_____

Contact Information:

_____ _____
Signature of HIPAA Compliance Officer
Printed Name: _____
Contact Information: