**HIPAA Compliance Status Questionnaire**

**Business Associate/Subcontractor**

The HIPAA Privacy, Security and Breach requirements extend beyond Covered Entities to all Business Associates and any downstream vendors or subcontractors that may come in contact with or otherwise have access to protected health information (PHI). Now a Business Associate or any subcontractor is individually responsible for compliance with HIPAA mandates for Privacy and Security.

To ensure compliance with HIPAA mandates, the first step is determining if an entity is subject to its PHI (ePHI) reach. The following Questionnaire will help a Covered Entity or a Business Associate determine if they are subject to HIPAA and help fashion appropriate programs to ensure compliance. Additionally, this Questionnaire will help the Covered Entity determine if the Business Associate is doing everything in their power to protect PHI.

\*Note, this is questionnaire can and should be revised according to each individual entity’s business interests. \*

**Part I. Business Associate Contact Information:**

|  |  |
| --- | --- |
| Company name: |  |
| Contact person: |  |
| Address: |  |
| Phone: |  |
| Email: |  |
| Fax: |  |
| Website: |  |

**Part II. Business Associate Information:**

|  |  |
| --- | --- |
| What type(s) of service do you provide to [Insert Covered Entity Name]? |  |
| Do the services you provide to [Insert Covered Entity Name] require the use or disclosure by, or to you, of PHI? |  |
| When did you sign your last BA agreement? |  |
| Where are your services carried out/performed? |  |
| What type of PHI do you access? |  |
| What form of PHI do you have access to or utilize in providing services to [Insert Covered Entity Name]? |  |
| What quantity of PHI do you access? |  |
| How do you access PHI? |  |
| How do you store PHI? |  |
| When did you complete your last HIPAA Risk Assessment? |  |
| If you use PHI off-site, do you access PHI through electronic means? |  |
| -If so, what safeguards are in place to protect the PHI? |  |
| Is any PHI maintained on portable media (flash drives or external hard-drives)? |  |
| How many employees do you have that have access to or use of [Insert Covered Entity Name] PHI? |  |
| At which locations do the employees access/ use [Insert Covered Entity Name] PHI? |  |
| Does your company use the PHI for purposes other than those for which you are a Business Associate? |  |
| -If yes, list the purposes for which data is being used or disclosed outside the purposes of the BAA? |  |
| Do you engage in any marketing activities in which PHI is used or disclosed in any manner? |  |
| Do you engage in any research activities in which PHI of [Insert Covered Entity Name] is used or disclosed? |  |
| -If so, please provide a detailed explanation of the policies and procedures in place regarding the use or disclosure of PHI for research purposes or append a copy of such policies and procedures to your response. |  |
| Do you have any processes or procedures regarding the de-identification of PHI? |  |
| -If so, please provide a detailed explanation or append a copy to this response. |  |
| Does your company use subcontractors in providing services to [Insert Covered Entity Name] under your agreement with [Insert Covered Entity Name]? |  |
| -If yes, do you have a chain-of-custody agreement or other written agreement that requires the subcontractor to meet the requirements of HIPAA? |  |
| Are any of the services you perform done outside of the jurisdiction of the United States? |  |
| -If yes, please list all other jurisdictions in which services are performed for [Insert Covered Entity Name]. |  |
| Do you store or maintain PHI for [Insert Covered Entity Name]? |  |
| -If yes, please describe the location(s) and manner in which PHI is stored or maintained and the security safeguards you have in place at each location. |  |
| Do you/your employees have direct contact with patients of [Insert Covered Entity Name]? |  |
| Has your company or any of your employees or subcontractors ever been involved in a data breach involving [Insert Covered Entity Name] PHI? |  |
| -If yes, how many breaches and how many patients were affected? |  |
| What steps were taken to mitigate the consequences and notify the affected patients and [Insert Covered Entity Name] of the breach? |  |

**Part III. HIPAA Compliance Checklist**

|  |  |
| --- | --- |
| Does your company have a HIPAA Compliance Program in place? |  |
| -If so, when was the Program last updated or reviewed? |  |
| Does your Program include separate policies on Privacy and Security pursuant to the HITECH statute and Rules? |  |
| -If so, please provide details on the same, including date created, type of policies and amendments. |  |
| Have you conducted a HIPAA Risk Analysis for Security and Privacy? |  |
| When was it conducted and who performed it? |  |
| Have you done vulnerability assessments of your network? |  |
| -If so, please provide details on the same, including date created, type of policies and amendments. |  |
| Are you required to create a Contingency Plan? |  |
| -If yes, have you created a Contingency Plan? [If the answer is yes, please respond to following 6 questions, if no, skip them.] |  |
| Have you conducted an Application & Data Criticality Analysis? (Print the analysis and submit it with the questionnaire.) |  |
| Have you created a Disaster Recovery Plan? (Print the analysis and submit it with the questionnaire.) |  |
| Have you created a Data Backup Plan? (Print the analysis and submit it with the questionnaire.) |  |
| Have you created an Emergency Mode of Operations Plan? (Print the analysis and submit it with the questionnaire.) |  |
| Have you created testing and revision procedures? |  |
| When was the last time you did an audit to determine your HIPAA compliance status? |  |
| Based on your knowledge, provide the date in which you became HIPAA complaint? |  |
| How often is staff trained & informed about your company’s HIPAA policies and programs? |  |
| When did you do your last staff training on HIPAA? |  |
| Which employees receive HIPAA training? |  |
| Were the HITECH updates to HIPAA included in the training? |  |
| Have other employees of your organization undergone comprehensive HIPAA training? |  |
| -If so, please list their name(s) and their title(s): |  |
| Are Executive Officers/ Board of Directors provided HIPAA training? |  |
| -If so, how often? Provide details of the course outline or append a copy of the materials to your response. |  |
| Are all employees of your organization provided basic HIPAA training? |  |
| -If so, how often? Provide details of the course outline. |  |

**Part III. Compliance Officer or Department**

|  |  |
| --- | --- |
| Does your company have a HIPAA Compliance Officer/Compliance Department? |  |
| -If so, please provide the name, title and email address for the HIPAA Compliance Officer. |  |
| Does your HIPAA compliance officer hold any HIPAA and/or Health care certifications, such as Certified HIPAA Privacy Security Expert (CHPSE), Certification in Healthcare Compliance (CHC), Certification in Healthcare Privacy Compliance (CHPC) or other similar certification? |  |
| -If yes, please list all certifications held and date of issuance. |  |
| -If not certified in HIPAA Compliance, what comprehensive HIPAA training has been undertaken by the HIPAA compliance officer? (Please provide date & duration of all the training.) |  |
| Has your company appointed a privacy and/or security officer? |  |
| -If so, please provide the Privacy officer’s name and email address. |  |
| Is the privacy officer an employee of your organization? |  |
| -If yes, is there a written job description regarding the Privacy Officer’s duties and responsibilities? |  |
| -If not an employee, is there a written contract between your Company and the Privacy officer regarding his/her duties and responsibilities? |  |
| Do you contract for other services that take place on your premises where the contractor’s employees work around PHI (i.e., janitorial services, duplication services, equipment leases and service providers)? |  |
| Do you rent or own your copier/fax machines or similar equipment that is used to copy, duplicate or transmit PHI? |  |
| Who handles your service calls for equipment utilized in your practice/business? |  |

\*Please provide copies of your Compliance Program, last risk assessment and other documentation regarding your HIPAA Compliance Program, policies and procedures.

By signing this document, you agree that you have answered all questions honestly and to the best of your knowledge.

**Part IV. Verification**

Signed by HIPAA Compliance Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed by Chief Executive Officer / Chief Financial Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed by Director/President: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_