Business Associate Security Questionnaire

[Organization] has identified you as a Business Associate. In order to meet our HIPAA Security Rule due diligence requirement to evaluate your safeguards of Protected Health Information (PHI), please complete this security questionnaire.

Business Name: _____

Date: _____

Primary Contact Name: _____

Title: _____

Phone: _____

E-mail: _____

Explain the service you will provide that involves you creating, maintaining, receiving, or transmitting ePHI on our behalf?

_____
_____

Administrative Safeguards:

Do you maintain an inventory of where PHI is used, disclosed, maintained, or transmitted?

_____

When did you conduct your last Risk Analysis?

_____

Were the risks identified mitigated or formally accepted?

_____

Has a formal contingency plan been adopted in case of a disaster? When was it last reviewed?

_____

Is ePHI stored or accessed on portable media (i.e. flash drive/CD/Laptop)?

_____

Describe your security measures taken to protect ePHI and attach your policies.

_____

What was the date of your last full back up performed?

_____

How often do you perform your backups?

_____

Is your backup stored off site?

_____

Is your backup stored in the USA?

_____

Is your backup encrypted/secured?

_____

What is your process to grant workforce members access to PHI? Attach your policy.

_____

Describe your process to terminate a workforce member's access to PHI and facility. Attach your policy.

_____

What is the date workforce members completed HIPAA security training?

_____

Physical Safeguards:

What is your process to destroy media containing PHI (CDs/Thumb drives/paper/hard drives)?

_____

Do you allow personal devices to be connected to the same network which contains ePHI?

_____

Are personally owned mobile devices approved and secure? How are they secured?

_____

Describe your security measures to prevent unauthorized physical access, tampering, and theft of PHI. Attach policy.

_____

Technical Safeguards:

What is your password policy regarding access to applications?

_____

Do users have unique user accounts to access ePHI?

_____

Do applications/systems automatically terminate after a period of inactivity? What is the timeframe?

_____

Do you grant users local administrative rights on their workstation?

_____

Do you use a wireless network? What security measures are in place?

_____

Do you send ePHI outside your network? What security measures do you have in place?

_____

Do you have a central repository for security events from applications, systems, and/or network devices?

_____

How often do you review your security events?

_____

Breach Notification:

Please provide your security incident response and breach notification policies.

_____

Have you appointed a security incident response team?

_____

Have you developed a security incident response plan? Please attach plan.

_____

When was the plan last tested?

_____

Third-Party Vendors (Sub-Contractors):

Do you use a third-party vendor who creates, maintains, receives, or transmit ePHI on your behalf?

_____

Has a formal contract been executed with the third-party vendor requiring the vendor to comply with the applicable privacy and security standards?

_____

How do you check your third-party vendor's security measures? When was it last checked?

_____

Who is the third-party vendor's HIPAA security contact? _____

Contact Number: _____

Return Questionnaire:

Please forward this questionnaire to:

[Organization]

[Full Address]

Documentation provided by:

Printed Name: _____

Signature: _____

Date: _____

Title: _____

Documentation reviewed by:

Printed Name: _____

Signature: _____

Date: _____

Title: _____

Follow up Audit Required: Yes _____

No _____