Business Associate Security Questionnaire

Shiawassee County Community Mental Health Authority (SCCMHA) has identified you as a Business Associate. In order to be compliant with the HIPAA Security Rule due diligence requirement to evaluate the safeguards of Protected Health Information (PHI) please complete this HIPAA/HITECH security questionnaire.

Business Associate Name:_____ Date: _____

Primary Contact Name:_____ Title: _____

Phone:_____ Fax:_____ E-mail: _____

What type of services do you provide to SCCMHA and how is PHI used, accessed, disclosed, transmitted and/or stored?

Administrative Safeguards

1. Do you maintain a PHI disclosure log? _____
2. When was the last risk assessment conducted? _____
   a. Have identified risks been mitigated or formally accepted? _____
3. Has a formal contingency plan been adopted in case of disaster? _____
   a. When was the last review/update? _____
4. Is ePHI stored or accessed on portable media (i.e. flash drive)? _____
   a. If yes, describe your security measures taken to protect ePHI and attach policies

      _____
5. What was the date of your last full back up performed? _____
   a. How often do you perform full back ups?_____
   b. Is your back up stored off site?_____
   c. Is your back up encrypted?_____
6. Describe your process or attach the policy and/or form to grant workforce members' access to PHI?

   _____
7. Describe your process or attach the policy and/or form to terminate workforce members' access to PHI and facilities?_____

   _____
8. Please provide the date employees and management underwent security training?_____
9. Were the applicable HITECH Act requirements included in the training? _____
10. Please attach a description of all security testing that has been performed over the past year.

Physical Safeguards

1. Please describe your measures to destroy items containing PHI (media, paper, hard drives)?

   _____

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

   _____

   _____
3. If so, are the personally owned mobile devices approved and secure? If so, how are the mobile devices secured?

   _____

4. Attach policies or describe security measures in place to prevent unauthorized physical access, tampering, and theft of PHI and ePHI.

Technical Safeguards

1. Please provide your password policy or describe how passwords are required for all applications that provide access to ePHI.
2. Do your systems automatically terminate after a period of inactivity? _____
    a. If so, what is the timeframe? _____
3. Do users have unique accounts to access ePHI? _____
4. Do you grant users local administrative rights on their workstations? _____
5. Do you use a wireless network? _____
    a. If yes, what measures do you have in place to secure ePHI?

    _____
6. Do you send ePHI outside your network? _____
    a. If yes, what measures do you have in place to protect ePHI sent outside your network?

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

    _____
8. If yes, when was the date they were last reviewed? _____
    a. How often are they reviewed? _____

Breach Notification

1. Please provide your security incident response and breach notification policies.
2. Have you appointed a security incident response team? ____
3. Have you developed a security incident response plan? ____
4. If yes, when was the plan last tested?

    _____

Third Party Vendors

Do you use any third party vendor that uses, discloses, transmits or stores PHI? _____

Third party vendor 1. (Name):_____ Contact Number: _____
Has a formal contract been executed with the third party vendor requiring the vendor comply with the HIPAA/HITECH Act privacy and security standards? _____
If so, how do you check your third party vendor's security measures?_____
What was date of the last time you checked the third party vendor's security measures?_____
Who is the third party vendor's HIPAA security contact?_____
Phone:_____

Third party vendor 2. (Name):_____ Contact Number: _____
Has a formal contract been executed with the third party vendor requiring the vendor comply with the HIPAA/HITECH Act privacy and security standards? _____
If so, how do you check your third party vendor's security measures?_____

What was date of the last time you checked the third party vendor's security measures?_____
Who is the third party vendor's HIPAA security contact?_____
Phone:_____

Third party vendor 3. (Name):_____ Contact Number: _____
Has a formal contract been executed with the third party vendor requiring the vendor comply with the HIPAA/HITECH Act privacy and security standards? _____
If so, how do you check your third party vendor's security measures?_____
What was date of the last time you checked the third party vendor's security measures?_____
Who is the third party vendor's HIPAA security contact?_____
Phone:_____

Please return this questionnaire along with your signed contract.

Documentation Provided By:

_____ _____
Signature Date

_____
Printed Name

_____
Title

Documentation Reviewed By:

_____ _____
Signature Date

_____
Printed Name

_____
Title