

ATTACHMENT H: HIPAA COMPLIANCE QUESTIONNAIRE

As a covered entity, it is the responsibility of the State Health Plan (Plan) to ensure its members' health information is protected from use and disclosures not allowed under the Health Insurance Portability and Accountability Act (HIPAA), as well as applicable state or federal laws.

The purpose of this form is to help the Plan evaluate HIPAA compliance of a prospective or current vendor who may request member data containing protected health information (PHI). The information provided here will help the Plan determine the vendor's level of understanding of HIPAA privacy and security rules, as well as their compliance status.

In order to be considered to do business with the Plan, the vendor must complete all questions and provide copies of all requested documentation. Any sensitive, trade secret, or proprietary answers or documentation provided in response to these questions shall be protected by the Plan in accordance with the confidentiality provisions of the solicitation document.

Vendor's Information:

Company name: _____

Address (city, state, and zip code): _____

Website URL: _____

Name of person completing form and role: _____

Email address: _____

Phone number: _____

Fax number: _____

NOTE:

- The contact information related to this questionnaire must be updated within 30 days of any personnel changes.
- If the space provided for any question is insufficient, include additional details on a separate page.

Compliance Checklist

1. Details of the individual responsible for HIPAA Compliance (if this designated position does not exist, provide the details of the employee who typically handles HIPAA privacy and security issues within your company or organization).

Name: _____

Title: _____

Address: _____

Phone number: _____

E-mail address: _____

Certification designation (e.g., CHC, CISSP, CIPP, CHP, CHPSE, etc.): _____

Date certified: _____

2. If the individual is not certified, provide detailed information regarding training that has been provided to the person responsible for HIPAA compliance (e.g., date last received training, name of company or person that provided training, etc.).

Employee HIPAA Training

3. Which employees receive HIPAA training? How frequently is their training refreshed?
4. Do all of the above employees receive comprehensive training (i.e. training which covers the privacy and security of PHI; both physical and technical)? Yes ☐ No ☐

If no, provide details of the level of training made available to employees.

5. When was HIPAA training last updated? When is the next planned update?

6. Are HIPAA privacy policies and procedures in place for employees to follow? Yes ☐ No ☐
7. Attach a copy of all privacy policies and procedures.
 - a. Indicate when the privacy policies were last reviewed or updated.
8. Are employees trained on the privacy policies and procedures? Yes ☐ No ☐
9. Are employees required to sign an attestation indicating they have read and understood the privacy policies and procedures? Yes ☐ No ☐
10. Are HIPAA security policies and procedures in place for employees to follow? Yes ☐ No ☐
11. Attach a copy of all HIPAA security policies.
 - a. Indicate when the security policies were last reviewed or updated.
12. Are employees trained on the security policies and procedures? Yes ☐ No ☐
13. Are employees required to sign an attestation indicating they have read and understood the HIPAA related security policies and procedures? Yes ☐ No ☐
14. Can you provide documentation that all applicable employees have completed training, upon request? Yes ☐ No ☐
15. Has your organization received any certifications regarding HIPAA compliance? Yes ☐ No ☐

If yes, provide copies of the certification and the date that the certification was awarded.
16. When was the last time your company was audited to determine HIPAA compliance? Provide date the audit was performed and the name of the company that performed it. Provide copies of the audit findings.

HIPAA Data Security

17. Provide details of the methods the company employs to secure and render PHI unusable, unreadable, or indecipherable to unauthorized individuals.
18. Describe security procedures – physical, technical, and administrative – in place to ensure the confidentiality of PHI internally, and when transmitting data externally to the Plan, to the Plan's pharmacy benefit management, or to vendors designated by the Plan.

19. Has the company conducted HIPAA Privacy and Security risk assessments and gap analyses in the last two (2) years? Yes ☐ No ☐

If yes, provide:

Date(s): Performed by:

What steps are in place to track and address all findings?

20. Provide the number of HIPAA violations reported to the Office of Civil Rights (OCR) in the last five (5) years, the details of the violation, and include the amount of the fine incurred (if any).

21. Does the company have procedures for the destruction of PHI compliant with the standards set by NIST? Yes ☐ No ☐

If yes, describe the procedure for that destruction.

Subcontractor Information

22. Does the company outsource work to subcontractors who would have access to Plan data and PHI? Yes ☐ No ☐

If yes, Provide the names of the companies, contact information, and details of what they are contracted to do.

23. Has the company entered into business associate agreements (BAAs) with all vendors who may qualify as "subcontractors"? Yes ☐ No ☐

If yes, provide copies of the executed BAAs.

24. How does the company enforce and monitor HIPAA policies with subcontractors/agents? What penalties or fixes are in place for violations?

25. In the last two (2) years, has your organization conducted audits of its subcontractors to verify compliance with applicable requirements?

Yes ☐ No ☐

If yes, provide the names of the companies audited, the dates the audits were conducted and details on whether any findings were identified.

Business Continuity Plan/Incident Response

26. Are there procedures to identify and respond to suspected or known security incidents, mitigate, to the extent possible, harmful effects of known security incidents, and document incidents and their outcomes?

Yes ☐ No ☐

If yes, describe:

27. Describe the company's business continuity plan in the event of a disaster (e.g., flood, fire, power failure, system failure).

- a. Provide the details of any incident(s) that that has required activating the business continuity plan within the last five (5) years.

I hereby certify that the information mentioned above is true and correct to the best of my knowledge and belief.

Name (Print)

Signature

Date