HIPAA Privacy/Data Security - Organization

1. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.1.) Does the provide not use or disclose PHI except as permitted or required in by Standard Contract 5.3 or law?

2. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.2.) Does the provider use the appropriate administrative safeguards in 45 CFR §164.308, physical safeguards in 45 CFR §164.310, and technical safeguards in 45 CFR §164.312; including policies and procedures regarding the protection of PHI in 45 CFR §164.316 and the provisions of training on such policies and procedures to applicable employees, independent providers, and volunteers, that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI Network Service Provider may create, receive, maintain or transmit on the Managing Entity and Department's behalf?

3. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.3.) Does the provider acknowledge that the foregoing safeguards, policies and procedures requirements apply to the Network Service Provider in the same manner as such requirements apply to the Managing Entity and Department; and the Network Service Provider and Subcontractors are directly liable under the civil and criminal enforcement provisions of §§13409 and 13410 of the HITECH Act, 45 CFR §§164.500 and 164.502(E) of the Privacy Rule (42 U.S.C. 1320d-5 and 1320d-6), as amended, for failure to comply with the safeguards, policies and procedures requirements and resulting U.S. Health and Human Services (HHS) guidance thereon?

4. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.4.) Does the provider report to the Managing Entity and Department any use or disclosure of PHI not permitted by 5.3, including breaches of unsecured PHI as required at 45 CFR §164.410, and any security incident?

5. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.5.) Does the provider notify the Managing Entity and Department's HIPAA Security Officer, HIPAA Privacy Officer, and Contract Manager within 120 hours after finding a breach or potential breach of personal and confidential data of the Department?

6. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.6.) Does the provider notify the Managing Entity and Department's HIPAA Privacy Officer and Contract Manager within 24 hours of HHS notification of any investigations, compliance reviews, or inquiries concerning violations of HIPAA?

7. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.7.) Does the provider provide additional information requested by the Managing Entity and/or the Department for investigation of or response to a breach?

8. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.8.) Does the provider provide at no cost: Notice to affected parties within 30 days of determination of any potential breach of personal or confidential data of the Managing Entity and/or Department (§501.171, F.S.); implementation of the Managing Entity and/or Department's prescribed measures to avoid or mitigate potential injury to any person due to a breach or potential breach of personal and confidential data of the Department; and, immediate actions limiting or avoiding recurrence of any breach or potential breach and any actions required by applicable federal and state laws and regulations regardless of the Managing Entity and/or Department's actions?

9. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.9.) For prior Contracts or other arrangements, does the Network Service Provider provide written certification its implementation complies with 45 CFR §164.532(d)?

HIPAA Privacy/Data Security - Organization

10. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.10.) Does the provider make PHI available in a designated record set to the Managing Entity and/or Department as necessary to satisfy the Managing Entity's and/or Department's 45 CFR §164.524 obligations?

11. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.10.) Does the provider make any amendment to PHI in a designated record set as directed or agreed to by the Managing Entity and/or Department per 45 CFR §164.526, or take other measures as necessary to satisfy the Managing Entity's and/or Department's 45 CFR §164.526 obligations?

12. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.12.) Does the provider maintain and make available the information required to provide an accounting of disclosures to a covered entity as needed to satisfy the Managing Entity's and/or Department's 45 CFR §164.528 obligations?

13. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.13.) To the extent the Network Service Provider carries any obligation under 45 CFR Subpart E, does the provider comply with the requirements of Subpart E that apply to the Managing Entity in the performance of that obligation?

14. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.3.14) Does the provider make internal practices, books, and records available to HHS for determining HIPAA rule compliance?

15. HIPAA Privacy & Data Security (LSF Standard Contract 5.3.6.a.i.) Does the provider provide the latest Departmental DCF HIPAA Basics Training to all persons prior to granting access to the Managing Entity and/or Department's information systems or any client or other confidential information?

16. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.1.) Does the provider designate an Information Security Officer competent to liaise with the Managing Entity and/or Department on security matters and maintain an appropriate level of information security for the Managing Entity and/or Department's information systems, or any client or other confidential information the Network Service Provider is collecting or using in the performance of this Contract?

17. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.1.) Does the Information Security Officer ensure that any access to the Managing Entity and/or Department information systems or any client or other confidential information is removed immediately upon such access no longer being required for Network Service Provider's performance under this Contract?

18. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.2.) Does the provider provide the latest Departmental Security Awareness Training to all persons prior to granting access to the Managing Entity and/or Department's information systems or any client or other confidential information?

19. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.3.) Does the provider require all persons granted access to comply with, and be provided a copy of CFOP 50-2, and will sign the Department's Security Agreement (Form CF 0112) annually?

20. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.3.) Does the provider prevent unauthorized disclosure or access, from or to Managing Entity and/or Department information systems or client or other confidential information. Clients of other confidential information on systems and network capable devices shall be encrypted per CFOP 50-2?

HIPAA Privacy/Data Security - Organization

21. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.4.) Does the provider notify the Network Manager within 120 hours, following the determination of any potential or actual unauthorized disclosure or access to the Department's information systems or to any client or other confidential information?

22. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.5.) Does the provider, at its own cost, comply with §501.171, F.S. (Security of confidential personal information)?

23. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.5.) Does the provider, at its own cost, implement measures deemed appropriate by the Managing Entity to avoid or mitigate potential injury to any person due to potential or actual unauthorized disclosure or access to Managing Entity and/or Department information systems or to any client or other confidential information?

24. HIPAA Privacy & Data Security (LSF Standard Contract 5.4.6.) Are the providers confidentiality procedures at least as protective as the most recent version of the Department's security policies and comply with any applicable professional confidentiality standards?

25. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.1.) Does the provider allow public access to all documents, papers, letters, or other public records as defined in §119.011(12), F.S., made or received by the Network Service Provider in conjunction with this Contract except that public records which are made confidential by law must be protected from disclosure?

26. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.1.) Does the provider maintain public records that ordinarily and necessarily would be required by the Managing Entity to perform the service?

27. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.2.) Does the provider, upon request from the Managing Entity's custodian of public records, provide to the Managing Entity a copy of requested records or allow the records inspected or copied within a reasonable time at a cost that does not exceed the cost provided in chapter 119, F.S., or as otherwise provided by law?

28. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.3.) Does the provider ensure public records exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law during this Contract term and following completion of this Contract if the Network Service Provider does not transfer the records to the Managing Entity?

29. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.4.) Does the provider upon completion of this Contract, transfer, at no cost, to the Managing Entity all public records in possession of the Network Service Provider or keep and maintain public records required by the Managing Entity to perform the service?

30. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.4.) If the Network Service Provider transfers all public records to the Managing Entity upon completion of this Contract, does the Network Service Provider destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements?

31. HIPAA Privacy & Data Security (LSF Standard Contract 5.5.2.4.) If the Network Service Provider keeps and maintains public records upon completion of this Contract, does the Network Service Provider meet all applicable requirements for retaining public records?