



HIPAA Privacy/Data Security - Organization

1. HIPAA Privacy & Data Security Org 01 (LSF Standard Contract 5.3.3.1.) Does the provider use or share protected health information (PHI) only as allowed or required by applicable HIPAA requirements and laws?
2. HIPAA Privacy & Data Security Org 02 (LSF Standard Contract 5.3.3.2.; 45 CFR §164.308, §164.312, and §164.316) Has the Network Service Provider and its subcontractors formally acknowledged and implemented policy and procedures to comply with all applicable HIPAA/HITECH privacy and security requirements, including understanding their direct liability for noncompliance?
3. HIPAA Privacy & Data Security Org 03 (LSF Standard Contract 5.3.3.3. §§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)) Does the provider have a policy and procedure that documents that it and any subcontractors must follow the same HIPAA, HITECH, privacy, security, and confidentiality requirements as the Managing Entity and the Department, and that they may be held directly liable for violations of these requirements?
4. HIPAA Privacy & Data Security Org 04 (LSF Standard Contract 5.3.3.4.; 45 CFR §164.410) Does the provider have a policy and procedure for reporting privacy breaches, unauthorized disclosures of protected health information (PHI), and security incidents to the Managing Entity and the Department?
5. HIPAA Privacy & Data Security Org 05 (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 Org 06 (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 Org 07 (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 Org 08 (LSF Standard Contract 5.3.3.8.; §501.171, F.S.) Does the provider have a policy and procedure to (1) notify affected individuals within 30 days of discovering a potential breach of personal or confidential information, (2) take steps to reduce potential harm, and (3) promptly correct the issue and prevent it from happening again?
9. HIPAA Privacy & Data Security Org 09 (LSF Standard Contract 5.3.3.9.) Does the provider ensure that all vendors, subcontractors, and other third parties that handle PHI on its behalf have written agreements requiring them to protect PHI and comply with the same privacy and security requirements as the provider?
10. HIPAA Privacy & Data Security Org 10 (LSF Standard Contract 5.3.3.10.; 45 CFR §164.524) Does the provider have a policy and procedure to provide requested PHI records to the Managing Entity and/or Department so individuals can access their health information when required?
11. HIPAA Privacy & Data Security Org 11 (LSF Standard Contract 5.3.3.11.; 45 CFR 164.526) Does the provider have a process to correct or update patient health information when requested by the Managing Entity and/or Department?



HIPAA Privacy/Data Security - Organization

12. HIPAA Privacy & Data Security Org 12 (LSF Standard Contract 5.3.3.12.; CFR §164.528) Does the provider maintain records of when patient health information (PHI) is disclosed and provide that information to the Managing Entity and/or Department when requested?
13. HIPAA Privacy & Data Security Org 13 (LSF Standard Contract 5.3.3.13.; 45 CFR Subpart E) Does the provider comply with all applicable HIPAA Privacy Rule requirements when performing responsibilities on behalf of the Managing Entity and/or Department?
14. HIPAA Privacy & Data Security Org 14 (LSF Standard Contract 5.3.3.14) Does the provider make its records, documentation, and compliance-related information available to federal regulators when requested to demonstrate compliance with HIPAA requirements?
15. HIPAA Privacy & Data Security Org 15 (LSF Standard Contract 5.3.6.a.i.) Before anyone receives access to Managing Entity or DCF systems, client information, or other confidential information, does the provider ensure that person completes the latest DCF HIPAA Basics training?
16. HIPAA Privacy & Data Security Org 16 (LSF Standard Contract 5.4.1.) Has the provider designated an Information Security Officer responsible for overseeing information security, approving and monitoring access to sensitive information and systems, and ensuring access is promptly removed when no longer needed?
17. HIPAA Privacy & Data Security Org 18 (LSF Standard Contract 5.4.2.) Does the provider ensure that all staff receive required security awareness training and sign required confidentiality and security agreements before being granted access to the Managing Entity's and/or Department's systems or confidential information?
18. HIPAA Privacy & Data Security Org 19 (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?
19. HIPAA Privacy & Data Security Org 20 (LSF Standard Contract 5.4.3.; CFOP 50-2) Does the provider have safeguards in place to prevent unauthorized access to or disclosure of confidential information, ensure confidential information stored on devices is encrypted, and require subcontractors to follow the same security requirements?
20. HIPAA Privacy & Data Security Org 21 (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?
21. HIPAA Privacy & Data Security Org 22 (LSF Standard Contract 5.4.5.; §501.171, F.S.) Has the provider established a policy and procedures to respond to actual or potential data breaches, mitigate harm, comply with applicable legal requirements, and ensure subcontractors comply with the same requirements?
22. HIPAA Privacy & Data Security Org 24 (LSF Standard Contract 5.4.6.) Does the provider have confidentiality policies and procedures that protect sensitive information at least as well as the Department's security requirements and applicable professional standards?



HIPAA Privacy/Data Security - Organization

23. HIPAA Privacy & Data Security Org 25 (LSF Standard Contract 5.5.1.; 119.011(12), F.S.) Does the provider make contract-related public records available when requested and protect confidential information that is not allowed to be disclosed?

24. HIPAA Privacy & Data Security Org 26 (LSF Standard Contract 5.5.2.1.) Does the provider maintain all public records necessary to perform services on behalf of the Managing Entity and make those records available as required?

25. HIPAA Privacy & Data Security Org 27 (LSF Standard Contract 5.5.2.2.) Does the provider have a policy and procedure for providing requested public records to the Managing Entity within a reasonable timeframe and at a cost allowed by law?

26. HIPAA Privacy & Data Security Org 28 (LSF Standard Contract 5.5.2.3.) Does the provider have a policy and procedures to protect confidential or exempt public records from unauthorized disclosure during and after the contract period, unless disclosure is permitted by law?

27. HIPAA Privacy & Data Security Org 29 (LSF Standard Contract 5.5.2.4.) Does the provider have a policy or procedure to transfer all required public records to the Managing Entity at the end of the contract, or retain those records in accordance with applicable record retention requirements, and provide electronic records in a compatible format when requested?