HIPAA Privacy/Data Security - Organization

1. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(7)(ii)(D) and (E)) Has the provider assessed relative criticality of specific applications and data in support of other contingency plan operations?

2. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(2) and 164.530(a)(1)(i)) Does the provider have an identified security official and designated a Privacy Officer who is responsible for development and implementation of data security policies and procedures required by HIPAA? These include policies and procedures to prevent, detect, contain, and correct security violations. ((This could be the same person))

3. HIPAA Privacy & Data Security Org (45 CFR 164.310(a)(2)(iii)) Has the provider implemented procedures for control and validation of access to facilities and/or to software based on his/her role or function, including visitor control, and control of access to software programs for testing and revision?

4. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(7)(ii)(D) and (E)) Has the provider implemented procedures for periodic testing and revision of contingency plans?

5. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(4)(ii)(B) and (C)) Health Care Clearinghouse Access Policies - Addressable.
If the provider is a hybrid organization with distinct and separate healthcare information function, has the provider implemented policies and procedures for granting access to PHI, and for establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process?

6. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(4)(ii)(A)) If the provider is a hybrid organization with distinct and separate healthcare information function, has the provider implemented policies and procedures that protect the PHI from unauthorized access by the larger organization? Required. See 45 CFR 164.105 for definitions.

7. HIPAA Privacy & Data Security Org (45 CFR 164.308(a)(7)(ii)(C)) Has the provider established (and implemented as needed) policies and procedures to enable continuation of critical business processes for protection and security of protected health information while operating in emergency mode?

8. HIPAA Privacy & Data Security Org Applicability Does the provider maintain a record of the movements of hardware and electronic media and any person responsible therefore?

9. HIPAA Privacy & Data Security Org Data Backup ((45 CFR 164.308(a)(7)(ii)(A))--) Does the provider create a retrievable, exact copy of PHI, when needed, prior to movement of equipment?

10. HIPAA Privacy & Data Security Org Data Backup (45 CFR 164.310(a)(2)(i)) Has the provider implemented procedures for allowing access to facility in support of data recovery under the disaster recovery and emergency management plan?

11. HIPAA Privacy & Data Security Org Data Backup (45 CFR 164.310(d)(2)(ii)) Media Re-use - Required.
Has the provider implemented policies and procedures to address removal of PHI from electronic media before the media are made available for reuse?

12. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.310(d)(2)(i)) Disposal of Media and Devices - Required.
Has the provider implemented policies and procedures to address final disposition of PHI and/or the hardware or electronic media on which it is stored?

HIPAA Privacy/Data Security - Organization

13. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.312(a)(2)(ii)) Emergency Access Procedure - Required.
Has the provider established and implemented as needed procedures for obtaining PHI during an emergency?

14. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.312(b)) Has the provider implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain and use PHI?

15. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.312(c)(2)) Mechanism to Authenticate Protected Health Information - Addressable.
Has the provider implemented electronic mechanisms to corroborate that PHI has not been altered or destroyed in an unauthorized manner?

16. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.312(e)(2)(ii)) Has the provider implemented electronic mechanisms to encrypt PHI whenever deemed appropriate?

17. HIPAA Privacy & Data Security Org Data Security Has the provider implemented procedures to verify that a person or entity seeking access to PHI is the one claimed?

18. HIPAA Privacy & Data Security Org Data Security Does the provider assign a unique name and/or number for identifying and tracking user identity?

19. HIPAA Privacy & Data Security Org Data Security (45 CFR 164.308(a)(5)(ii)) Security Awareness - Addressable.
Has the provider implemented periodic security updates; procedures for guarding against, detecting, and reporting malicious software; procedures for monitoring log-in attempts and reporting discrepancies; and procedures for creating, changing, and safeguarding passwords?

20. HIPAA Privacy & Data Security Org Incidents (45 CFR 164.308(a)(6)(ii)) Has the provider implemented policies and procedures to address security incidents, including identifying and responding to suspected or known security incidents, mitigating harmful effects of incidents, and documenting security incidents and outcomes?

21. HIPAA Privacy & Data Security Org Info Sys (45 CFR 164.308(a)(1)(ii)(D)) Did the provider implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports?

22. HIPAA Privacy & Data Security Org Risk Management (45 CFR 164.308(a)(1)(ii)(B)) Did the provider implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

23. HIPAA Privacy & Data Security Org Sanctions-1 (45 CFR 164.308(a)(1)(ii)(C)) Does the provider have appropriate sanctions to take against members of the workforce who fail to comply with HIPAA privacy policy, procedures, requirements?

24. HIPAA Privacy & Data Security Org Security (45 CFR 164.310(b)) Has the provider implemented policies and procedures that specify proper functions to be performed, the manner in which functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of

workstations that can access protected health information?

25. HIPAA Privacy & Data Security Org Security (45 CFR 164.310(c)) Has the provider implemented physical safeguards for all workstations that access protected health information, to restrict access to authorized users?

26. HIPAA Privacy & Data Security Org Security (45 CFR 164.312(a)(2)(iii)) Has the provider implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity?

27. HIPAA Privacy & Data Security Org Security (45 CFR 164.312(e)(2)(ii)) Has the provider implemented electronic mechanisms to encrypt protected health information whenever deemed appropriate? (Provider should be able to demonstrate or describe the software or mechanism used to encrypt PHI for transmittal.)

28. HIPAA Privacy & Data Security Org Security (45 CFR 164.310(a)(2)(ii)) Has the provider implemented procedures to safeguard facility and equipment from unauthorized access, tampering and theft? (This should be physically observed as well as reported by the NSP)

29. HIPAA Privacy & Data Security Org Security (45 CFR 164.310(a)(2)(iv)) Has the provider implemented procedures for documenting repairs and modifications to physical components of facility related to security?

30. HIPAA Privacy & Data Security Org Supervision (45 CFR 164.308(a)(3)(ii)(C)) Did the provider implement procedures for terminating access to protected health information when employment of a workforce member ends, or when responsibilities change as specified in the Workforce Clearance Procedure?