LCBHS

Lake County Behavioral Health Services

Behavioral Health Compliance Section

Contractor Risk Assessment Review
FY 2021-22 Monitoring Instrument

| | | | |
|---|---|---|---|
| Contracting Agency: | | | |
| Administrator: | | | |
| Physical Address: | | | |
| Phone: | | | |
| Email: | | | |
| Review Analyst: | | | |
| Review Date: | | | |
| Date of Last Review: | | Review Type: | ☐ Site ☐ Desk |
| Current Risk: | ☐ Low ☐ Med ☐ High | Previous Risk: | ☐ Low ☐ Med ☐ High |
| Approving Supervisor: | | Approval Date: | |
| Approving Supervisor Signature: | | | |

# INSTRUCTIONS:

All contracted providers are required to complete the left hand column titled “Plan Question & regulation” unless directed otherwise. The provider is required to return the completed risk assessment (tool) along with the appropriate supporting evidence, to the LCBHS Analyst. Please label the supporting evidence with the corresponding question number (e.g. Question # with the document name). If the County is scheduled for a site review, the County’s responses will be discussed at that time. If the County is scheduled for a desk review, the Analyst will evaluate the completed instrument and supporting evidence, and will email follow-up questions for further clarification.

# SCORING KEY:

Each question is scored individually for risk. The score is based on risks to clients, the County and to the provider. Each question will be given a score of Pass, Conditional Pass, or Fail. Conditional Pass and Fail will include documented reasons for selection.

**DESIGNATION OF RISK**

| RISK ASSESSMENT | | YES | NO |
|---|---|---|---|
| 1. | Has the County's key staff changed since last review? (Key staff include: Project manager, fiscal lead, and/or program lead?) | ☐ | ☐ |
| Position: | | | |
| 2 | Were the County's financial reports incomplete, inaccurate and/or late? (quarterly expenditure reports, year-end cost report) | ☐ | ☐ |
| 3 | Did the County have significant findings in last year's audit? | ☐ | ☐ |
| 4. | Has the organization identified all EPHI? This includes EPHI that provider created, receive, maintain or transmit. Please note that EPHI may be resident on computer workstations, servers or on portable devices such as laptops, and PDAs. | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| RISK ANALYSIS § 164.308(a)(1)(ii)(A) - *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."* | | | |
| 5. | Are security measures are already in place to protect EPHI – this can be a comprehensive view of all measures, whether administrative, physical or technical, such as an overarching security policy; door locks to rooms where EPHI is stored; or the use of password protected files. | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| RISK MANAGEMENT §164.308(a)(1)(ii)(B) - *"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."* | | | |
| 6. | Provider developed, applied and implemented policies specific to violations of the security policies and procedures? If so, do they provide appropriate sanctions for workforce members who fail to comply with your security policies and procedures? (i.e., have you included your sanction policy in your workforce manual and trained your staff on the policy?) | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| SANCTION POLICY § 164.308(a)(1)(ii)(C) - "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity." | | | |
| 7. | Are the procedures used by the workforce consistent with provider's access policies (i.e., do people who should have access actually have that access? Are people who should not have access prevented from accessing the information?) | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| AUTHORIZATION AND/OR SUPERVISION § 164.308(a)(3)(ii)(A) - "Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed." | | | |

| | | | |
|---|---|---|---|
| 8. | Are contracts in place with outside entities entrusted with health information generated by the provider's office? If so, do the contracts provide assurances that the information will be properly safeguarded? For example, if contracted with a software vendor for the internal practice management system, what assurances does the provider have that the vendor's products are HIPAA compliant? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| WRITTEN CONTRACT OR OTHER ARRANGEMENTS § 164.308(b)(4) - *"Document the satisfactory assurances required by this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [(the Business Associate Contracts or Other Arrangements Standard)]."* | | | |
| 9. | Does the provider office have a method of destroying EPHI on equipment and media you are no longer using? For example, has provider considered purchasing hard drive erasure software for a planned upgrade of office computers? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| DISPOSAL § 164.310(d)(2)(i) - *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."* | | | |
| 10. | Do office policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| *This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required* | | | |
| 11. | Does the provider office have a method of destroying EPHI on equipment and media you are no longer using? For example, has provider considered purchasing hard drive erasure software for a planned upgrade of office computers? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| DISPOSAL § 164.310(d)(2)(i) - *"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."* | | | |
| 12. | Does the provider have a process in place to assign each user of their system a unique user identifier? If so, can the identifier be used to track user activity within information systems that contain EPHI? This may or may not be reasonable or appropriate for a solo clinician where access has been granted to all office staff. | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| UNIQUE USER IDENTIFICATION § 164.312(A)(2)(I) - *"Assign a unique name and/or number for identifying and tracking user identity."* | | | |
| 13. | Do the current information systems have an automatic logoff capability to ensure that unauthorized users do not access data on unattended workstations? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |

| | | | |
|---|---|---|---|
| AUTOMATIC LOGOFF § 164.312(a)(2)(iii) - *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."* | | | |
| 14. | Does the system require the input of something known only to the person or entity seeking access to EPHI, (such as a password or PIN) prior to granting the requested access? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| *This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required (R).* | | | |
| 15. | Based on the required risk analysis, is encryption needed to protect the transmission of EPHI between the office and outside organizations? If not, what measures are in place to ensure the protection of this information? Some small providers might consider password protection of documents or files containing EPHI and/or prohibiting the transmission of EPHI via email. | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| ENCRYPTION § 164.312(e)(2)(ii) - *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."* | | | |
| 16. | Does a policy and procedure exist to assess potential risks and vulnerabilities to confidentiality and integrity? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| | | | |
| 17. | Does the provider have a current, established back-up and disaster recovery plan?? | ☐ | ☐ |
| ☐ | Supporting Documentation (Policy, Procedure, Proof of Practice) | | |
| | | | |

**Scoring Key:**

Count the number of YES responses: _____

| | | | | |
|---|---|---|---|---|
| 0-4 Yes | Provider is considered low risk – Desk/Onsite alternative | LOW | | |
| 5-8 Yes | Provider is considered medium risk – Desk/Onsite alternative | | MED | |
| 9-17 Yes | Provider is considered high risk –Onsite Review | | | HIGH |