



JENNIFER KENT  
DIRECTOR

State of California—Health and Human Services Agency  
Department of Health Care Services



EDMUND G. BROWN JR.  
GOVERNOR

June 21, 2017

Sent via e-mail to: karenstockton@co.modoc.ca.us

Karen Stockton, Director  
Modoc County Health Services  
441 North Main Street  
Alturas, CA 96101

SUBJECT: State Fiscal Year (SFY) 2016-17 - County Monitoring Unit Report

Dear Director Stockton:

Enclosed are the results of Modoc County's 2016-17 Substance Abuse Prevention and Treatment (SAPT) Block Grant (BG)<sup>1</sup>, and the State County Contract compliance review. The Department of Health Care Services (DHCS) is responsible for monitoring requirements of the SAPT BG and the terms of the State County Contract operated by Modoc County.

The County Monitoring Unit (CMU) within the Performance Management Branch (PMB) of DHCS performed a comprehensive review based on responses to the monitoring instrument, discussion with county staff, supporting documentation and requirements. The enclosed report addresses and/or identifies compliance deficiencies, required corrective actions, advisory recommendations, and referral for technical assistance.

Modoc County is required to submit a Corrective Action Plan (CAP) addressing each deficiency noted to the CMU Analyst by July 21, 2017. The CAP must follow the guidelines detailed within the attached report. Please reference the enclosed CAP instructions and e-mail the CAP to the CMU Analyst. Supporting CAP documentation may be e-mailed or mailed to the address listed below. If you have any questions regarding this report or need assistance, please contact the CMU analyst.

Sincerely,

Trang Huynh  
CMU Analyst  
(916) 650-0529  
[Trang.huynh@dhcs.ca.gov](mailto:Trang.huynh@dhcs.ca.gov)

---

<sup>1</sup> Title 45 Code of Federal Regulations, Part 96, Subpart L – Substance Abuse Prevention and Treatment Block Grant requirements



**County Monitoring Unit Report**  
Modoc County

Distribution:

To: Karen Stockton, Director, Modoc County Health Services

CC: Victoria King-Watson, Substance Use Disorder Program, Policy and Fiscal Division, Assistant Division Chief  
Tracie Walker, Performance Management Branch, Section Chief  
Patrick Daglia, Fiscal Management and Accountability Branch, Section Chief  
Denise Galvez, Policy and Prevention Branch, Section Chief  
Sandy Yien, Program Support and Grants Management Branch, Section Chief  
Susan Jones, County Monitoring Unit, Supervisor  
Cynthia Hudgins, Drug Medi-Cal Monitoring Unit I, Supervisor  
Stephanie Quok, Drug Medi-Cal Monitoring Unit II, Supervisor  
Danielle Stumpf, Office of Women, Perinatal and Youth Services, Supervisor  
Tiffany Stover, Postservice Postpayment Unit I, Supervisor  
Janet Rudnick, Postservice Postpayment Unit II, Supervisor  
Trudi Romero, Policy and Prevention Branch, Office Technician  
Tara Sheperd, MA, CAS Deputy Director, AOD Administrator, Modoc County Health Services  
Brian Bernard, Program Manager, Modoc County Health Services

Date: June 21, 2017

Report Prepared by: *Trang Huynh, County Monitoring Analyst*  
Manager Approval: *Susan Jones, County Monitoring Supervisor*

---

**Lead CMU Analyst:**  
Trang Huynh

**Review Date:** June 6-8, 2017

**Assisting CMU Analyst(s):**  
Eric Painter

**Review Period:** SFY 2016-17

**County:** Modoc

**County Address:**  
441 North Main Street  
Alturas, CA 96101

The Department of Health Care Services (DHCS) is required to provide programmatic, administrative, and fiscal oversight of the statewide Substance Abuse Prevention and Treatment Block Grant (SAPT BG), the State County Contract, and Drug Medi-Cal (DMC) Substance Use Disorder (SUD) services through annual compliance reviews.

This report summarizes the findings of the compliance review conducted by the County Monitoring Unit (CMU).

## CORRECTIVE ACTION PLAN

Pursuant to the State County Contract, Exhibit A, Attachment I, Part V, Section 4, 7, (a-b) each deficiency identified must be addressed via a Corrective Action Plan (CAP). The CAP is due within thirty (30) calendar days of the date of this monitoring report. Advisory recommendations are not required to be addressed in the CAP.

The Corrective Action Plan shall:

1. Address each programmatic deficiency;
2. Provide a specific description of how the deficiency will be corrected;
3. Identify the staff person responsible for correcting the deficiency and ensuring future compliance;
4. Specify the target date for complete implementation of each deficiency; and
5. As deficiencies are corrected, include training documentation, revised policies/procedures, and other materials which demonstrate the correction of a deficiency, if applicable.

The CMU analyst will monitor progress of CAP implementation until complete.

## REVIEW SCOPE

- I. Regulations:
  - a. 22 CCR § 51341.1 – Drug Medi-Cal Substance Use Disorder Services
  - b. 9 CCR, Division 4, Chapter 4, Subchapter 1 – 6: Narcotic Treatment Programs
  - c. 45 CFR; Part 96; Subpart L; §96.121 through 96.137: Substance Abuse Prevention and Treatment Block Grant
  - d. 42 USC, Section 300x-21 through 300x-66: Substance Abuse Prevention and Treatment Block
  - e. HSC, Division 10.5, Section 11750 – 11970: State Department of Health Care
  
- II. Program Requirements:
  - a. State Fiscal Year (SFY) 14/15 - 16/17 State County Contract, herein referred to as State County Contract
  - b. State of California *Youth Treatment Guidelines Revised August 2002*
  - c. DHCS *Perinatal Services Network Guidelines FY 2016-17*
  - d. National Culturally and Linguistically Appropriate Services (CLAS)
  - e. Alcohol and Drug Program (ADP) Bulletins
  - f. Mental Health and Substance Use Disorders Services (MHSUDS) Information Notices

## 1.0 ADMINISTRATION

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 2.0 SAPT BG MONITORING

After review of the program's protocols, policies and procedures, no deficiencies were cited.

### ADVISORY RECOMMENDATIONS:

#### **AR 2.18:**

State County Contract Exhibit A, Attachment I, Part IV, Section 3, A, 1, (a-e)

*Contractor's performance under this Exhibit A, Attachment I A2, Part IV, shall be monitored by the State during the term of this Contract. Monitoring criteria shall include, but not be limited to:*

- (a) Whether the quantity of work or services being performed conforms to Exhibit B A2;*
- (b) Whether the Contractor has established and is monitoring appropriate quality standards;*
- (c) Whether the Contractor is abiding by all the terms and requirements of this Contract;*
- (d) Whether the Contractor is abiding by the terms of the Perinatal Services Network Guidelines (Document 1G); and*
- (e) Contractor shall conduct annual onsite monitoring reviews of services and subcontracted services for programmatic and fiscal requirements.*

*Contractor shall submit copy of their monitoring and audit reports to DHCS within two weeks of issuance. Reports should be sent by secure, encrypted e-mail to:*

*[sudcountyreports@dhcs.ca.gov](mailto:sudcountyreports@dhcs.ca.gov); or*

*Substance Use Disorder - Prevention, Treatment and Recovery Services  
Division, Performance Management Branch, Department of Health Care Services,  
PO Box 997413, MS-2627  
Sacramento, CA 95899-7413*

**Recommendation:** It is recommended that the County individualize each of the 15 Culturally and Linguistically Appropriate (CLAS) Standards in the County's monitoring tool.

### 3.0 DRUG MEDI-CAL

The following DMC deficiencies in regulations, standards, or protocol requirements were identified:

#### COMPLIANCE DEFICIENCIES:

##### **CD 3.26:**

State County Contract Exhibit A, Attachment I, Part V, Section 4 B-2 (a)

*Contractor shall ensure that all Subcontractors receive training on the requirements of Title 22 regulations and DMC requirements at least annually. Documented attendance of any subcontracted provider at the annual trainings offered by DHCS (specified in Section 4, paragraph (A) (3) of this contract) shall suffice to meet the requirements of this provision. Contractor shall report compliance with this section to DHCS annually as part of the DHCS County monitoring process.*

**Finding:** The County did not provide current Title 22 training materials.

##### **CD 3.27:**

State County Contract Exhibit A, Attachment I, Part V, Section 2 B-1 (a)

*... Contractor shall have a documented system for monitoring and evaluating accessibility of care, including a system for addressing problems that develop regarding waiting times and appointments.*

**Finding:** The County did not provide a copy of policies and procedures in place for monitoring and evaluating system of care, including a system for addressing problems that develop regarding waiting times and appointments.

#### ADVISORY RECOMMENDATIONS:

##### **AR 3.30:**

State County Contract Exhibit A, Attachment I, Part V, Section 4, B, 4(a)

*(a) All complaints received by Contractor regarding a DMC certified facility shall be forwarded to:*

*Drug Medi-Cal Complaints are to be submitted to:  
Department of Health Care Services  
P.O. Box 997413  
Sacramento, CA 95899-7413  
Call the Hotline  
Phone Toll-Free: (800) 822-6222*

**Recommendation:** The County should use the specific address to notify DHCS when complaints regarding a DMC certified facility are received.

**AR 3.33:**

State County Contract Exhibit A, Attachment I, Part V, Section 4, A, 2, (b)

*...If programmatic or fiscal deficiencies are identified, the Provider shall be required to submit a Corrective Action Plan (CAP) the Contractor for review and approval prior to submission to DHCS for final approval.*

State County Contract Exhibit A, Attachment I, Part V, Section 4, A, 2, (b), i

*Pursuant to CCR, Title 22, Section 51341.1(o), all deficiencies identified by the PSPP review, whether or not a recovery of funds results, must be corrected and the entity that provided the services must submit a Contractor-approved CAP to the PSPP Unit within 60 days of the date of the PSPP report.*

State County Contract Exhibit A, Attachment I, Part V, Section 4, A, 2, (b), i, 1, d

*Identify who will be responsible for correction and who will be responsible for on-going compliance.*

**Recommended:** Even though the County has not experienced a Postservice Postpayment (PSPP) CAP, the County should have a process in place to identify the timeline for PSPP reviews, and responsible party for ensuring the PSPP CAPs are reviewed and approved.

## 4.0 PERINATAL

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 5.0 ADOLESCENT/YOUTH TREATMENT (AYT)

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 6.0 FISCAL AUDITING

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 7.0 PRIMARY PREVENTION

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 8.0 CULTURAL COMPETENCE

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 9.0 ELECTRONIC HEALTH RECORDS (EHR)

After review of the program's protocols, policies and procedures, no deficiencies were cited.

## 10.0 CALIFORNIA OUTCOMES MEASUREMENT SYSTEM TREATMENT (CalOMS Tx)

The following deficiencies in CalOMS and DATAR regulations, standards, or protocol requirements were identified:

### COMPLIANCE DEFICIENCIES:

#### **CD 10.57.d:**

State County Contract, Exhibit A, Attachment I, Part III, F, (3)

*Contractor shall comply with the treatment and prevention data quality standards established by the State. Failure to meet these standards on an ongoing basis may result in withholding non-DMC funds.*

**Finding:** The County's annual updates or client discharges, for beneficiaries in treatment over one year, were not submitted.

## 11.0 PRIVACY AND INFORMATION SECURITY

The following deficiencies in Privacy and Information Security regulations, standards, or protocol requirements were identified:

### COMPLIANCE DEFICIENCIES:

#### **CD 11.60:**

State County Contract, Exhibit G-3, Attachment A, 1, A

**Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.

**Finding:** The County did not demonstrate that all workforce members completed annual privacy and security training.

#### **CD 11.69:**

State County Contract, Exhibit G-3, Attachment A, 3, A

**System Security Review.** Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

**Finding:** The County does not conduct an annual system risk assessment/security review.

#### **CD 11.76:**

State County Contract, Exhibit G-2, 3, B, 2-3

2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

- a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;

- b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and*
- c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment I and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.*

**Finding:** The County does not meet all the requirements to protect Department PI.

**CD 11.76.a:**

State County Contract, Exhibit G-2, 3, B, 2-3

2) **Safeguards.** *To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.*

3) **Security.** *Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:*

- a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;*
- b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and*
- c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment I and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in*

*Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.*

**Finding:** The County does not have written policies and procedures implemented, that addresses information privacy and security for PI.

**CD 11.76.b:**

State County Contract, Exhibit G-2, 3, B, 2-3

2) **Safeguards.** *To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.*

3) **Security.** *Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:*

- a. *Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;*
- b. *Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and*
- c. *If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment I and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.*

**Finding:** The County's information privacy and security, policy and procedure does not include a section regarding security for PI.

**CD 11.76.c:**

State County Contract, Exhibit G-2, 3, B, 2-3

2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

- a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;
- b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
- c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment I and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.

**Finding:** The County did not provide a copy of the requested policies and procedures which address PI.

**CD 11.78:**

State County Contract, Exhibit G-1,13 (a-c)

Exhibit G-2, 9 (a-c)

*Breaches and Security Incidents.* During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

- a. **Initial Notice to the Department.** (1) To notify the Department immediately by telephone call or email or fax upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department within 24 hours (one

hour if SSA data) by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this ExhibitG-1, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Information Protection Unit (916.445.4646, 866-866-0602) or by emailing ([privacyofficer@dhcs.ca.gov](mailto:privacyofficer@dhcs.ca.gov)). Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS information Security Officer website ([www.dhca.ca.gov](http://www.dhca.ca.gov), then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link [www.dhca.ca.gov/privacy](#). Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI, Contractor shall take:

- i) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - ii) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- a. **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Information Protection Unit.
- b. **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

**Finding:** The County did not demonstrate a process in place for reporting breached or security incidents that include:

- Notifying DHCS immediately by telephone, e-mail, or fax
- Notifying DHCS within 24 hours of a suspected security incident
- Utilizing “Privacy Security Incident Report” form
- Submitting “Privacy Incident Report” form within 72 hours
- Providing a complete report within 10 working days of breach or disclosure

**ADVISORY RECCOMENDATIONS:**

**AR 11.74:**

State County Contract, Exhibit G-1, 3, D, 2-3

2) **Compliance with the HIPAA Security Rule.** *To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 CFR Sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR Section 164, subpart C, in compliance with 45 CFR Section 164.316. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor’s operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.*

3) **Security.** *Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:*

- a. Complying with all of the data system security precautions listed in Attachment A, Data Security Requirements;*
- b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement; and*
- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A- 130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.*

**Recommendation:** The County should update their policies and procedures, which addresses PHI privacy and security, with a current signature and date.

## 12.0 TECHNICAL ASSISTANCE

The County did not request any TA during the site review for SFY 16-17.