Schedule 12.1.1 – Information Privacy and Security, Criminal Offender Record Information, California Law Enforcement Telecommunication Systems, and County Facility Access

Table of Contents

1. OVERVIEW

A. This Schedule 12.1.1 is intended to protect the privacy and security of specified County information that Contractor may receive, access, store, maintain or transmit, under this Agreement, and to comply with the applicable federal and State laws and regulations governing the access, use and disclosure of the specified County information. The County information subject to the requirements of this Schedule consists of:

1. Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and
2. Personal Information (PI) as defined under the California Civil Code Section 1798.3. PI may include data provided to the County by the State of California or by the Social Security Administration (SSA); and
3. Personally Identifiable Information (PII) as defined under the Information Exchange Agreement (IEA) between the State of California and the SSA dated October 11, 2014, which incorporates the Computer Matching and Privacy Protection Agreement (CMPPA) between the SSA and the State of California's Health and Human Services Agency dated July 2, 2014; and
4. Criminal Offender Record Information (CORI) as defined by California Penal Code sections 11075 and 13102, including information from the California Law Enforcement Telecommunications System (CLETS), the County of San Diego Probation Case Management System (PCMS), and local County records.
5. This Schedule does not reduce any other obligation set forth in the Agreement or any other law or regulation governing the information. To the extent another provision of the Agreement requires different protection of information subject to the requirements of this Schedule, the provisions requiring greater protection of the information shall prevail.

B. This Schedule consists of the following parts:

1. Section 1, Business Associate Agreement;
2. Section 2, Privacy and Security of PI and PII;
3. Section 3, Data Security Requirements; and
4. Section 4, CORI/CLETS; and
5. Section 5, Miscellaneous.

C. Definitions: Capitalized terms used in this Section 1, and for which no definition in this Section 1 is provided, shall be defined as otherwise defined in the Agreement. Terms used, but not otherwise defined, in this Section 1 shall have the same meaning as those terms as are defined in 45 Code of Federal Regulations (CFR) section 160.103 and 164.501. (All regulatory references in this BAA are to Title 45 of the CFR unless otherwise specified.)

1 "Breach"

1.2 For Sections 1 and 2 of this Exhibit 12.1.1, "Breach" shall have the same meaning given to such term under HIPAA.

1.3 For purposes of Section 3 of this Exhibit 12.1.1, "Breach" "Breach" shall have the same meaning given to such term under the IEA and CMPPA. It shall include a "PII loss," as defined in the CMPPA, and both a "Breach of the security of the system" and a "Notice Triggering Personal Information" event, as identified in CIPA (Civil Code section 1798.29).

2 "Business Associate" shall have the same meaning as the term under HIPAA, and for purposes of this Agreement, shall mean the Contractor. "Contractor Employees" shall mean, for purposes of this Schedule 12.1.1, Contractor's officers, directors, employees, volunteers and interns.

3 "CORI" shall mean records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release (Cal. Pen. Code sections 11075 and 13102). CORI includes but is not limited to information from the CLETS, PCMS, and local County records.

4 "County Hybrid Entity" shall mean that part of County designated as the hybrid entity subject to the Standards for Privacy of Individually Identifiable Health Information set forth in sections 160 and Part 164, Subparts A and E and those parts of County designated as business associates of other entities subject to the Standards for Privacy of Individually Identifiable Health Information set forth in Parts 160 and 164, Subparts A and E.

5 "County PHI" shall have the same meaning as "Protected Health Information" (PHI) below, specific to PHI received from, or accessed, created, stored, maintained, transmitted, used, disclosed, or received by Contractor, or its subcontractors and agents, on behalf of County, under this Agreement.

6 "County PII/PI" shall have the same meaning as Personally Identifiable Information/Personal Information as below, specific to PII/PI received by Contractor from County or acquired or created by Contractor in connection with performing the functions, activities, and services specified in this Section 2 on County's behalf.

7 "Covered Entity" shall generally have the same meaning as the term "covered entity" at section 160.103, and for purposes of this BAA, shall mean County-Hybrid Entity.

8 "HIPAA" means collectively the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164.

9 "Individual" shall have the same meaning as the term ''individual'' in section 164.501 and shall include a person who qualifies as a personal representative in accordance with section 164.502(g).

10 "Personal Information" shall have the same meaning given to such term in CIPA, section 1798.3(a).

11 "Personally Identifiable Information" (PII) shall have the same meaning given to such term in the IEA and the CMPPA.

12 "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in section 164.501 and is limited to information created or received by Contractor from or on behalf of County.

13 "Required by law" shall have the same meaning as the term ''required by law'' in section 164.501.

14"Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

15 "Security incident" means the attempted and successful unauthorized access, use, disclosure, modification, or destruction of County PHI, County PI or PII, confidential data, or interference with system operations in an information system that processes, maintains or stores County PHI.

16 "Unsecured PHI" shall have the meaning given to such term under HIPAA and, 42 U.S.C., section 17932(h), and any guidance issued pursuant to such regulations.

2. BUSINESS ASSOCIATE AGREEMENT

2.1. Recitals

2.1.1. This Section 1, Business Associate Agreement ("BAA") constitutes a Business Associate relationship as that term is defined and used in HIPAA.

2.1.2. The County may, from time-to-time, disclose to the Contractor certain information pursuant to the terms of this BAA, some of which may constitute PHI, including PHI in electronic media under federal law.

2.1.3. As set forth in this BAA, Contractor, hereafter, is the Business Associate of County, acting on County's behalf and providing services, or performing or assisting in the performance of activities on County's behalf, which may include accessing, creation, receipt, storing, maintenance, transmittal, use or disclosure of PHI.

2.2. Contractor Responsibilities

2.2.1. General Obligations

2.2.2. Permitted Uses and Disclosures of County PHI by Contractor. Contractor shall only use County PHI as required by the Agreement or as required by law. Any such use or disclosure shall, to the extent practicable, be limited to the limited data set as defined in section 164.514(e)(2), or if needed, to that which is minimally necessary to accomplish the intended purpose of such use or disclosure in compliance with HIPAA.

2.2.3. Except as otherwise limited in this Agreement, Contractor may use or disclose County PHI on behalf of, or to provide services to, County for the purposes set forth in the Agreement, if such use or disclosure of PHI would not violate HIPAA if done by County.

2.2.4. Except as otherwise limited in the Agreement, Contractor may use County PHI to provide Data Aggregation services to County as permitted by sections 164.504(e)(2)(i)(B).

2.2.5. Prohibited Uses and Disclosures

2.2.6. Contractor shall not disclose County PHI to a health plan for payment or health care operations purposes if County PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the Individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and HIPAA.

2.2.7. Contractor shall not directly or indirectly receive remuneration in exchange for County PHI, except with the prior written consent of County and as permitted by 42 U.S.C. section 17935(d)(2).

2.2.8. Safeguards

2.2.8.1. Contractor shall comply with HIPAA regarding any and all operations conducted on behalf of County under this Contract and shall use appropriate safeguards that comply with HIPAA to prevent the unauthorized use or disclosure of County PHI.

2.2.8.2. Contractor shall develop and maintain a written information privacy and security program that complies with HIPAA, and that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

2.2.9. Security. Contractor shall ensure the continuous security of all computerized data systems and paper documents containing County PHI. These steps shall include, at a minimum:

2.2.9.1. Comply with all Standards put forth in Section 3, Data Security Requirements, of this Schedule 12.1.1;

2.2.9.2. Achieve and maintain compliance with HIPAA; and

2.2.9.3. Provide 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 as otherwise required by the Agreement.

2.2.10. Mitigation of Harmful Effects. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI by Contractor, Contractor's Employees, Contractor's agents, Contractor's subcontractors or Contractor's vendor, and/or in violation of the requirements of the Contract.

2.2.11. Contractor's Agents, Subcontractors and Vendors. Contractor shall ensure that any agent, subcontractor or vendor to whom it provides County PHI, imposes the same conditions on such agents, subcontractors and vendors that apply to Contractor with respect to County PHI under this BAA, and that comply with all applicable provisions of HIPAA, including requirements that such agents, subcontractors and vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect County PHI. Contractor shall incorporate, when applicable, the relevant provisions of this BAA into each subcontract to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured County PHI be reported to Contractor.

2.2.12. In accordance with section 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by any agent, subcontractor or vendor of the agreement between Contractor and the agent, subcontractor and vendor, Contractor shall:

2.2.12.1. Provide an opportunity for the agent, subcontractor or vendor to end the violation and terminate the agreement if the agent, subcontractor or vendor does not end the violation within the time specified by County; or

2.2.12.2. Immediately terminate the agreement if the agent, subcontractor or vendor has violated a material term of the agreement and cure is not possible.

2.2.13. Availability of Information to County. Contractor shall provide access to County PHI at the request of County, in the time and manner designated by County, pursuant to section 164.526.

2.2.14. Contractor shall use the forms and processes developed by County for this purpose and shall respond to all requests for access to records requested by County within forty-eight (48) hours of receipt of such request by producing records or verifying that there are none.

2.2.15. Contractor shall make internal practices, books, and records relating to the use and disclosure of County PHI received from, or created or received by Contractor on behalf of County available to County, or at the request of County to the Secretary, in a time and manner designated by County or the Secretary.

2.2.16. Cooperation with County. Contractor shall cooperate and assist County to the extent necessary to ensure County's compliance with the applicable terms of HIPAA, such as, but not limited to:

2.2.16.1. Documentation of Disclosures. Contractor shall document disclosures of County PHI and make these disclosures available to County in accordance with HIPAA, including but not limited to sections 164.528, and 42 USC section 17935, and in the time and manner designated by County.

2.2.16.2. If Contractor maintained electronic health records as of January 2009, when requested, Contractor shall provide an accounting of disclosures including those for Treatment, Payment, and Healthcare Operations (TPO). If Contractor acquired electronic health records for County after January 1, 2009, or acquires electronic records for County, when requested, Contractor shall provide an accounting of disclosures, including those for TPO, effective with disclosures on or after the date the electronic health record was or is acquired, or on or after January 1, 2011, whichever date is later.

2.2.16.3. The electronic accounting of disclosures shall include the three (3) years prior to the request for an accounting. Contractor shall provide to County, in the time and manner designated by County, but no more than sixty (60) calendar days after County's request, an accounting of disclosures necessary to meet the requirements in section 164.528.

2.2.16.4. Reporting of Unauthorized Use or Disclosure. Contractor shall implement reasonable systems for the discovery of and prompt reporting to County of any use or disclosure of County PHI not allowed for by the Agreement and/or any transmission of unsecured County PHI. Contractor shall provide all reports of unauthorized uses or disclosures simultaneously to the COR and County Privacy Officer.

2.2.17. Initial Report

2.2.17.1. Contractor shall notify County COR and County Privacy Officer immediately by telephone call and by email upon the discovery of a breach of unsecured County PHI in electronic media or in any other media if County PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the SSA.

2.2.17.2. Contractor shall notify County COR and County Privacy Officer by email within twenty-four (24) hours of the discovery of any suspected security incident, breach or loss of County PHI.

2.2.17.3. A suspected security incident or breach shall be treated as discovered by Contractor or its agent, subcontractor or vendor as of the first day the breach or security incident is known, even if it is not confirmed, or by exercising reasonable diligence would have known, to any person (other than the person causing or committing the security incident or breach) who is a Contractor Employee or agent, subcontractor or vendor of Contractor.

2.2.17.4. Reporting shall additionally include emailing to the County COR and County Privacy Officer of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall report using the form attached hereto as Exhibit 12.1.1-1.

2.2.17.5. Investigation and Investigation Report. Contractor shall immediately investigate such security incident, breach, or unauthorized access, use or disclosure of County PHI. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report" to County COR and County Privacy Officer.

2.2.17.6. Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "County 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 and applicable federal and State law. 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. The report shall be submitted to the County COR and County Privacy Officer. If County requests information in addition to that listed on the "County Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and, appropriate, approve the determination of whether a breach occurred, Individual notifications are required, and the corrective action plan is adequate. County action or inaction in determining whether a breach occurred, the need for notifications or any correction shall not relieve Contractor of any federal or State requirements with which Contractor must comply.

2.2.18. Responsibilities for Notification of Breaches. If County determines that the cause of a breach of County PHI is attributable to Contractor, Contractor Employees or Contractor's subcontractors, agents or vendors, Contractor shall notify Individuals of the breach or unauthorized use or disclosure when notification is required under federal or State law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirements that:

2.2.18.1. Notifications be made to Individuals without unreasonable delay and in no event later than sixty (60) calendar days from the date the breach was discovered. County shall approve the time, manner and content of any such notifications before notifications are made.

2.2.18.2. Notifications shall be made to media outlets and to the Secretary, if a breach of unsecured County PHI involves more than five-hundred (500) residents of the State of California or its jurisdiction. County shall approve the time, manner and content of any such notifications before notifications are made.

2.2.18.3. Nothing in this Schedule 12.1.1 shall limit or reduce Contractor's indemnification or other responsibilities set forth in the Agreement, nor shall anything in this Schedule 12.1.1 reduce or limit Contractor's liability to County or any third party as set forth in the Agreement.

2.2.18.4. Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PHI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

2.2.19. Designation of Individuals

2.2.19.1. Contractor shall designate a privacy officer to oversee its data privacy program who shall be responsible for carrying out the requirements of this Agreement and for communicating on Privacy matters with County.

2.2.19.2. Contractor shall designate a security officer to oversee its data security program who shall be responsible for carrying out the requirements of this Agreement and for communicating on security matters with County.

2.2.20. County Responsibilities. County shall not request Contractor to use or disclose County PHI in any manner that would not be permissible under HIPAA if done by County.

3. PRIVACY AND SECURITY OF PERSONAL INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

3.1. Recitals

3.1.1. The purpose of this Section 2 of Schedule 12.1.1 is to set forth Contractor's Privacy and Security obligations with respect to PI and PII that the Contractor may access, create, receive, maintain, use, store or disclose for or on behalf of County pursuant to this Agreement. Specifically, this Section 2 applies to PI and PII that is not PHI, and therefore, is not addressed in Section 1, the Business Associate Agreement, of this Schedule 12.1.1. To the extent that data is both PHI and PI, or both PHI and PII, both Sections 1 and 2 of this Schedule 12.1.1 govern its use.

3.1.2. The IEA requires County to extend the IEA's terms to contractors who receive data provided to County from the SSA, or data provided to County from the SSA through the State. If Contractor receives such data from County, Contractor must comply with the IEA.

3.2. Contractor Responsibilities

3.2.1. Permitted Uses and Disclosures of County PII/PI by Contractor. Contractor shall only use County PII/PI to perform functions, activities, or services for or on behalf of County pursuant to this Agreement, provided that such use or disclosure does not violate any applicable federal or State law or regulation.

3.2.2. Confidentiality of Alcohol and Drug Abuse records. Contractor shall comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter 1, Subchapter A, Part 2, as applicable.

3.2.3. Prohibited Uses and Disclosures. Contractor shall not use or disclose County PII/PI, other than as permitted or required by the Agreement or as permitted or required by law.

3.2.4. Safeguards

3.2.4.1. Contractor shall use appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of County PII/PI and to prevent use or disclosure of County PII/PI, other than as provided for by the Agreement.

3.2.4.2. Contractor shall develop and maintain a written information privacy and security program that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

3.2.5. Security. Contractor shall take any and all steps necessary to ensure the continuous safety of all data systems containing County PII/PI. The Contractor shall, at a minimum:

3.2.5.1. Comply with all of the data system security precautions listed in Section 3 of this Schedule 12.1.1, Data Security Requirements; and

3.2.5.2. Provide 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

3.2.5.3. Provide a level and scope of security that is no less than otherwise provided by the Agreement; and

3.2.5.4. If the data includes County PII, Contractor shall also comply with the Privacy and Security requirements in the CMPPAA and the IEA.

3.2.6. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PII/PI by Contractor or its agents, in violation of this Schedule 12.1.1.

3.2.7. Contractor's Employees, Agents, Subcontractors and Vendors. Contractor shall ensure that any Contractor Employee, agent, subcontractor or vendor that accesses, creates, receives, maintains, stored, uses, discloses, receives or transmits County PII/PI on behalf of the Contractor shall adhere to the same restrictions, conditions, and requirements that apply to the Contractor. Contractor shall incorporate, when applicable, the relevant provisions of this Schedule 12.1.1 into each subcontract or sub-award to such agents, subcontractors and vendors, including the requirements related to security incidents or breaches of unsecured County PII/ PI.

3.2.8. Availability of Information. Contractor shall make County PII/PI available to County for purposes of oversight, inspection, amendment, and response to request for records, injunctions, judgments, and orders for production of County PII/PI. Contractor shall provide a list of all Contractor Employees, subcontractors, vendors and agents who have access to County PII/PI, including employees, agents and vendors of its subcontractors, agents and vendors, at the request of County. Contractor shall provide any requested records to County within forty-eight (48) hours of such request.

3.2.9. Internal Practices. Contractor shall make internal practices, books, and records relating to the use and disclosure of County PII/PI received from, or created or received by Contractor on behalf of County available to County, in a time and manner designated by County. Confidentiality shall not prevent County, its agents, or any other governmental entity from accessing such records if that access is legally permissible under the applicable federal or State regulations.

3.2.10. Cooperation with County. Contractor will cooperate and assist County, in the time and manner designated by County, to ensure County's compliance with applicable federal and State laws and regulations, such as, but not limited to CIPA. Contractor's cooperation shall include, but is not limited to: accounting of disclosures, correction of errors, production, disclosures of a security breach, and notice of such breach to affected individuals that involve County PII/PI and Contractor.

3.2.11. Reporting of Breaches and Security Incidents. Contractor shall implement reasonable systems for the discovery of, prompt reporting to County of, and prompt corrective action regarding any use or disclosure, or suspected use or disclosure, of County PII/PI not provided for by the Agreement and/or any transmission of unsecured County PII/PI and shall take the following steps:

3.2.11.1. Contractor shall make all reports required by this Section 2 of breaches and security incidents simultaneously to County COR and County Privacy Officer.

3.2.11.2. Initial Reporting

3.2.11.2.1. Reporting shall be immediate, by both telephone and email, upon the discovery of a breach of unsecured County PII/PI in electronic media or in any other media if County PII/PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the SSA.

3.2.11.2.2. Reporting shall be within twenty-four (24) hours by email of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/ PI in violation of this Section 2, or potential loss of confidential data affecting this Section 2.

3.2.11.2.3. A breach or suspected security incident shall be treated as discovered by Contractor as of the first day on which the breach is known, even if not confirmed, 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 the Contractor.

3.2.11.2.4. Reporting shall additionally include emailing of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall use the form attached hereto as Exhibit 12.1.1-1. Investigation and Investigation Report. Contractor shall immediately investigate such security incident or breach. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report."

3.2.11.2.5. Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "County 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 federal and State law. 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 County requests information in addition to that listed on the "County Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and approve the determination of whether: a breach occurred, individual notifications are required, and the corrective action plan is adequate.

3.2.11.2.6. Responsibility for Reporting Breaches. If County determines that the cause of a breach of County PII/PI is attributable to Contractor, Contractor Employees, or Contractor's subcontractors, agents or vendors, Contractor is responsible for all required reporting as specified under CIPA section 1798.29(a) and as may be required under IEA, as well as any other federal or State law and shall pay any costs of such notifications, as well as any costs associated with the breach. County shall approve the time, manner, and content of any such notifications and County's review and approval must be obtained before the notifications are made. If the Contractor believes duplicate reporting of the same breach or incident may occur, because its subcontractors or agents may report the breach or incident to County as well, Contractor shall notify County and may take action to prevent duplicate reporting.

3.2.12. Nothing in this Schedule 12.1.1 shall limit or reduce Contractor's indemnification or other responsibilities set forth in the Agreement, nor shall anything in this Schedule 12.1.1 reduce or limit Contractor's liability to County or any third party as set forth in the Agreement.

3.2.13. Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/PI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

3.2.14. Designation of Individuals. Contractor shall appoint Privacy and Security officials who are accountable for compliance with this Section 2 and for communicating Privacy and Security matters to County.

4. DATA SECURITY REQUIREMENTS

4.1. Contractor shall ensure the continuous security of all data systems and paper documents containing County PHI and/or County PII/PI. The security obligations set forth herein are in addition to those set forth in the Agreement, and shall not lessen or decrease Contractor's security obligations. These steps shall include, at a minimum:

4.2. Personnel Controls. Contractor shall ensure that all workforce members who assist in the performance of functions or activities on behalf of County, or access or disclose County PHI and/or County PII/PI, shall:

4.2.1. Have undergone a thorough Contractor background check, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security, privacy, or integrity of County PHI and/or County PII/PI, prior to the workforce member obtaining access to County PHI and/or County PII/PI. The Contractor shall retain each workforce member's Contractor background check documentation for a period of three (3) years following contract termination.

4.2.2. Complete privacy and security training, at least annually, at Contractor's expense. Each of Contractor's Employees, and Contractor's agents, subcontractors and vendors and their employees, who receive information privacy and security training shall sign a certification, indicating the person's name and the date on which the training was completed. These certifications shall be retained for a period of six (6) years following contract termination, and shall be available to County upon request.

4.2.3. Sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to County PHI and/or County PII /PI and shall be renewed annually. The Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following contract termination. The form of the Confidentiality Statement is attached hereto as Exhibit 12.1.1-2.

4.2.4. Be appropriately sanctioned if they fail to comply with security and privacy policies and procedures, including termination of employment when appropriate.

4.3. Physical Security Controls. Contractor shall safeguard County PHI and/or County PII/PI from loss, theft, inadvertent disclosure, and therefore shall:

4.3.1. Ensure County PHI and/or County PII/PI is used and stored in an area that is physically safe from access by unauthorized persons during both working hours and nonworking hours;

4.3.2. Secure all areas of Contractor facilities where Contractor workers use or disclose County PHI and/or County PII/PI. The Contractor shall ensure that these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or other access authorization, and access to premises is by official identification;

4.3.3. Issue Contractor Employees who assist in the administration of County PHI and/or County PII/PI identification badges and require Contractor Employees to wear badges at facilities where County PHI and/or County PII/PI is stored or used;

4.3.4. Ensure each location where County PHI and/or County PII/PI is used or stored has procedures and controls that ensure an individual whose access to the facility is terminated:

4.3.4.1. Is promptly escorted from the facility by an authorized Contractor Employee; and

4.3.4.2. Immediately has their access revoked to any and all County PHI and/or County PII/PI.

4.3.5. Ensure there are security guards or a monitored alarm system twenty-four (24) hours a day, seven (7) days a week at facilities where County PHI and/or County PII/PI is stored;

4.3.6. Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI and/or County PII/PI have perimeter security and access controls that limit access to only authorized Information Technology Staff. Visitors to the data center area must be escorted by authorized Contractor Employees at all times;

4.3.7. Store paper records with County PHI and/or County PII/PI in locked spaces in any facilities that are multi-use, meaning that there are County PHI and/or County PII/PI functions and Contractor functions in one building in work areas that are not securely segregated. The contractor shall have policies that state Contractor Employees shall not leave records with County PHI and/or County PII/PI unattended at any time in cars or airplanes and shall not check County PHI and/or County PII/PI on commercial flights; and

4.3.8. Use all reasonable means to prevent non-authorized personnel and visitors from having access to, control of, or viewing County PHI and/or County PII/PI.

4.4. Technical Controls. Contractor shall ensure that:

4.4.1. All workstations and laptops that process and/or store County PHI and/or County PII/PI shall:

4.4.1.1. Be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk; and

4.4.1.2. Install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

4.4.1.3. Apply critical security patches. There shall be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. All applicable patches shall be installed within thirty (30) days of vendor release.

4.4.1.4. All servers containing unencrypted County PHI and/or County PII/PI shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

4.4.1.5. Only the minimum necessary amount of County PHI and/or County PII/PI required to perform necessary business functions may be copied, downloaded, or exported.

4.4.1.6. All electronic files that contain County PHI and/or County PII/PI shall be encrypted when stored on any removable media or portable device (i.e. flash drives, cameras, mobile phones, CD/DVD, backup media, etc). Encryption shall be a FIPS 140-2 certified algorithm, which is 128bit or higher, such as AES.

4.4.1.7. All users shall be issued a unique user name for accessing County PHI and/or County PII/PI. Username shall be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours.

4.4.1.8. Passwords shall be:

4.4.1.8.1. At least eight characters;

4.4.1.8.2. A non-dictionary word;

4.4.1.8.3. Changed at least every ninety (90) days;

4.4.1.8.4. Changed immediately if revealed or compromised; and

4.4.1.8.5. Composed of characters from at least three of the following four groups from the standard keyboard:

4.4.1.8.6. Upper case letters (A-Z)

4.4.1.8.7. Lower case letters (a-z)

4.4.1.8.8. Arabic numerals (0-9)

4.4.1.8.9. Non-alphanumeric characters (punctuation symbols)

4.4.1.9. Passwords shall not be shared and shall not be stored in readable format on the computer.

4.4.1.10. Appropriate management control and oversight, in conjunction with County of the function of authorizing individual user access to County PHI and/or County PII/PI and over the process of maintaining access controls numbers and passwords.

4.4.1.11. When no longer needed, all County PHI and/or County PII/PI shall be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

4.4.1.12. All systems providing access to, transport of, or storage of County PHI and/or County PII/PI shall:

4.4.1.12.1. Provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

4.4.1.12.2. Display a warning banner stating: i) that the data that may be accessed is confidential, ii) that the systems accessed are logged, and iii) that authorized users' use of PHI/PII/PI data is exclusively for County business purposes. Users must be directed to log off the system if they do not agree with these requirements. If County provides a warning banner to be implemented by Contractor, Contractor's implementation shall satisfy this requirement except to the extent that Contractor is otherwise obligated to provide a warning banner for its business purposes.

4.4.1.12.3. Maintain an automated audit trail that identifies the user or system process which initiates a request for County PHI and/or County PII/PI, or which alters County PHI and/or County PII/ PI. The audit trail shall be date and time stamped, shall log both successful and failed accesses, shall be read only, and shall be restricted to authorized users. If County PHI and/or County PII/ PI is stored in a database, database logging functionality shall be enabled. Audit trail data shall be archived for at least three (3) years after occurrence, and shall be available to County upon request.

4.4.1.12.4. Use role based access controls for all users, enforcing the principle of least privilege.

4.4.1.12.5. Be protected by a comprehensive intrusion detection and prevention solution if they are accessible via the internet.

4.4.1.12.6. All data transmissions of County PHI and/or County PII/PI outside the secure internal network shall be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing County PHI and/or County PII/PI can be encrypted. This requirement pertains to any type of County PII/PI in motion such as website access, file transfer, and E-Mail.

4.5. Audit Controls. Contractor shall ensure:

4.5.1. All systems processing and/or storing County PHI and/or County PII/PI shall 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.

4.5.2. All systems processing and/or storing County PHI and/or County PII/PI shall have a routine procedure in place to review system logs for unauthorized access.

4.5.3. All systems processing and/or storing County PHI and/or County PII/PI shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4.5.4. Investigate anomalies in usage of County PHI and/or County PII/PI identified by County and report conclusions of such investigations and remediations to County.

4.6. Business Continuity / Disaster Recovery Controls

4.6.1. Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic County PHI and/or County PII/PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

4.6.2. Contractor shall ensure Data Centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI or PII/PI, must include sufficient environmental protection such as cooling, power, fire prevention, detection, and suppression.

4.6.3. Contractor shall have established documented procedures to backup County PHI and/or County PII/PI to maintain retrievable exact copies of County PHI and/or County PII/PI. The plan shall include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore County PHI and/or County PII/PI should it be lost. At a minimum, the schedule shall be a weekly full backup and monthly offsite storage of County data.

4.7. Paper Document Controls. Contractor shall ensure:

4.7.1. County PHI and/or County PII/PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or separate office inside a larger office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI and/or County PII/PI in paper form shall not be left unattended at any time in vehicles and shall not be checked in baggage during commercial flights.

4.7.2. Visitors to areas where County PHI and/or County PII/PI are contained shall be escorted and County PHI and/or County PII/PI shall be kept out of sight while visitors are in the area.

4.7.3. County PHI and/or County PII/PI shall be disposed of through confidential means, such as cross cut shredding and pulverizing.

4.7.4. County PHI and/or County PII/PI shall not be removed from the premises of the Contractor except for identified routine business purposes or with express written permission of County.

4.7.5. Faxes containing County PHI and/or County PII/PI shall not be left unattended and fax machines shall be in secure areas. Fax cover sheets shall contain a confidentiality statement instructing persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

4.7.6. Mailings of County PHI and/or County PII/PI shall be sealed and secured from damage or inappropriate viewing of County PHI and/or County PII/PI to the extent possible. Mailings which include 500 or more individually identifiable records of County PHI and/or County PII/PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of County's Privacy Officer to use another method is obtained.

4.7.7. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI and/or County PII/PI by Contractor or its agents, including a subcontractor, and/or in violation of the requirements of the Agreement.

5. CORI/CLETS REQUIREMENTS

5.1. Application. This Section 4, CORI/CLETS Requirements, applies to all Contractor employees, agents and subcontractors with access or potential access to CORI systems including those individuals with only unescorted access to County facilities/properties that store, process or transmit CORI/CLETS information in order to ensure the safety of program offenders and the integrity of this program. Access, or potential access to CORI/CLETS, can be in the form of hardcopy documentation, verbal communication, or other forms of information sharing, as well as access to Probation's facilities where CORI/CLETS is created, stored, handled or discussed.

5.2. Training Requirements. Contractor shall ensure that all Contractor Employees, agents and subcontractors, with physical and logical access to CORI and/or the facilities that secure CORI systems (unless these individuals are escorted by authorized personnel at all times) shall receive CORI/CLETS training from a certified CLETS/National Crime Information Center (NCIC) within six (6) months of assignment to this Agreement and biennially thereafter, in accordance with FBI Criminal Justice Information Services Security Policy (FBI CJIS) section 5.2 and California CLETS Policies, Practices and Procedures (PPP)section 1.8.3.A.4. CORI/CLETS training, which will include laws, policies, and consequences regarding access to, and use of, criminal offender record information, will be provided by the Probation Department if needed.

5.3. Training Reporting. A list of all persons with "physical and logical" access to CORI, his or her title, e-mail address and phone number(s) must be sent to the COR with the person's last date of training. Contractor shall complete the CORI/CLETS Training Request Form (Exhibit 12.1.1-2) for all employees, agents, volunteers, and subcontractors that have not received CORI/CLETS training or are required to renew his or her training. Contractor shall forward this list and form, within 30 days of employee, agent, volunteer and/or subcontractor assignment, to the Probation Department, 9444 Balboa Avenue, Suite 500, San Diego, CA 92123 Attention: Contracts Unit.

5.4. CORI/CLETS Clearance Requirements. In addition to the background check requirements of the Agreement, Contractor shall ensure that background checks are required and completed by all Contractor Employees, subcontractors, agents and vendors with access to CORI/CLETS information, systems and its facilities as provided under section 5.12 of the FBI CJIS and section 1.9.2 of the PPP.

5.4.1. At a minimum, the following background checks shall be completed and approved prior to performance under this Agreement:

5.4.1.1. Criminal background clearance through the Probation Department (Background Division), State of California Department of Justice (DOJ) and Federal Bureau of Investigation (FBI);

5.4.1.1.1. Out-of-State Background Checks: Contractor shall request a "hard card" from Probation for each out-of-state Contractor Employee, Subcontractor, agent or vendor, and Probation will provide to Contractor a "hard card" from the FBI. Each individual shall take the "hard card" to a local law enforcement agency, get fingerprinted and submit the cards to Probation at the following location: 9444 Balboa Avenue, Suite 500, San Diego, CA 92123, Attn: Background Division. Probation will then send the cards to the State Department of Justice, which will conduct both DOJ and FBI background checks.

5.4.1.2. Driving record through the State of California Department of Motor Vehicle (DMV);

5.4.1.3. Drug testing.

5.4.1.4. Background check packages must be submitted to the Probation Department located at 9444 Balboa Avenue, Suite 500, San Diego, CA 92123 Attention: Background Division. The Contractor is advised to keep copies of all applications/background check packages submitted to the Probation Department.

5.4.1.5. Incomplete Packages will not be accepted. A typical background package includes:

5.4.1.6. A complete signed Security Clearance Request Form,

5.4.1.7. A clean, valid, and legible copy of Social Security Card or Social Security Administration abstract,

5.4.1.8. A clean, valid and legible copy of a Driver's license, or State-issued Identification Card,

5.4.1.9. For Contractor Employees who are not citizens of the United States: either a valid Resident Alien Badge or valid form of picture identification,

5.4.1.10. For Contractor Employees requesting electronic access authorization: a complete Access Registration Form

5.4.1.11. Contractors are required to submit one check covering the cost of the background check process for all employees. The check should be made payable to: County of San Diego. Questions regarding associated costs should be directed to the COR.

5.4.1.12. If applicable, Contractor must have completed Livescan applications for each Contractor Employee, agent, subcontractor, vendor and their employees in addition to the background package. Contractor shall obtain a Livescan application from the Probation Department. County may provide Contractor with information on various Livescan locations and fees. A fee is required by the Department of Justice and collected by the Livescan operator. Contractor shall pay all Livescan associated fees.

5.4.1.13. Background checks generally take 4-6 weeks to process. The Probation Department will notify Contractor directly, or through the COR, the results of submitted background checks. If the background screening results are acceptable, Contractor Employee may begin services under the Agreement.

5.4.1.14. Results of Criminal Background Clearance. If a background check indicates a criminal record inappropriate to be assigned to this Agreement, that individual shall not be assigned to perform services under the Agreement.

5.4.2. Inappropriate Criminal Record. An inappropriate criminal record may include, but is not limited to:

5.4.2.1. Felony convictions of any kind;

5.4.2.2. Convictions of crimes of moral turpitude (prostitution, sex offenses, etc.);

5.4.2.3. Exhibiting patterns of criminal behavior;

5.4.2.4. Exhibiting patterns of anti-social behavior;

5.4.2.5. Convictions for illegal immigrant smuggling;

5.4.2.6. Outstanding warrants and/or unresolved investigations;

5.4.2.7. A misdemeanor conviction;

5.4.2.8. More than three Failure to Appear citations within the last two years;

5.4.2.9. Receipt of subsequent arrest notices after approval and issuance of access to CORI/CLETS and/or a County facility, and/or

5.4.2.10. As otherwise required by federal and state law, including but not limited to Section 5.12 of the FBI Criminal Justice Information Services Security Policy and Section 1.9.2 of the California CLETS Policies, Practices and Procedures (PPP).

5.4.3. Review of Violations. County shall evaluate any Penal Code or other statutory violations individually and make a determination as to whether the violation precludes an individual's ability to efficiently carry out Agreement functions.

5.4.4. Removal of Employees, Volunteers or Subcontractors. Contractor shall immediately remove a Contractor Employee or agent, subcontractor or vendor from duties related to the Agreement if the updated clearance indicates a criminal record inappropriate to be assigned to the Agreement.

5.4.5. Duration of Background Checks. Background checks for Contract Employees and subcontractors, agents and vendors shall be valid for five years. Background reinvestigations shall be conducted every five years unless Rap Back is implemented. ("Rap Back" is a national fingerprint and criminal history system maintained by the FBI CJIS Division service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.)

5.4.6. Department of Motor Vehicles (DMV). Contractor shall obtain and review the DMV record of any of Contractor's Employees who are assigned to the Agreement and whose job duties include, or may include, driving. Such Contractor Employees are referred to in this section as "Drivers." Contractor shall enroll in the State of California's DMV Employer Pull Notice Program (EPN) and ensure that all staff are added and enrollment properly maintained. The EPN Program can be found at: Employer Pull Notice Program - California DMV.

5.4.6.1. Drivers shall have no more than three violation points for traffic violations, at fault accidents, and misdemeanor convictions within the last year. As stated in the Vehicle Code, Section 12810.5, "four or more points in 12 months…shall be prima facie presumed to be a negligent operator of a motor vehicle."

5.4.6.2. All Drivers shall maintain a valid California Driver License. Exceptions must be approved by the COR on a case-by-case basis prior to employment of contract staff.

5.4.7. Drug Testing. Contractor shall cause Contractor Employees assigned to the Agreement to undergo drug testing. No person shall be assigned to the Agreement who tests positive for any illegal drugs, including marijuana. Contractor shall also comply with County of San Diego Board of Supervisors Policy C-25, which can be found at: http://www.sdcounty.ca.gov/cob/policy/ .

5.4.7.1. Contractor shall subsequently conduct reasonable-suspicion testing of Contractor Employees as deemed necessary by Contractor.

5.4.8. Tuberculosis Testing. Contractor shall cause Contractor Employees assigned to the Agreement, and having direct contact with minors, to undergo annual testing for tuberculosis. Contractor may retest a Contractor Employee who tests positive for tuberculosis. Contractor may, in cases where a Contractor Employee has falsely tested positive in the past, accept a letter from the employee's physician that states that the employee is not exhibiting symptoms of active tuberculosis that would warrant additional x-rays and examination. Any Contractor Employee who is confirmed to have infectious tuberculosis shall not be assigned to Agreement functions where the Contractor Employee may come into contact with minors.

5.4.9. Contractor Employee, Agent, Subcontractor and Agent References. Contractor shall obtain and verify personal and prior employment references where available from Contractor Employees, subcontractors, agents and vendors assigned to the Agreement. Contractor shall evaluate any negative references and determine whether any such information precludes the employee from carrying out the functions of the Agreement.

5.4.10. Education Requirements. Contractor shall confirm compliance with education requirements as specified in the Agreement.

5.4.11. Exceptions. Exceptions to compliance with the aforementioned clearance requirements must be approved by the COR on a case-by-case basis.

5.4.12. Employee/Volunteer Statement. Per PPP section 1.5.1, all contractor employees, agents, volunteers and subcontract personnel with "physical and logical" access to CORI/CLETS shall sign the Employee/Volunteer Statement Form (Exhibit 12.1.1-3).

5.5. Maintenance of Records. Maintenance of CORI/CLETS Training Records: Parties shall maintain records of all training, testing, and proficiency affirmation of CORI/CLETS in accordance with section 1.8.3.A.3 of the PPP and shall be made available for inspection, upon request, by the other party.

5.6. Changes to Access. Contractor shall notify Probation of any changes in writing or email for Contractor Employees, agents, subcontractors or vendors assigned to the Agreement within thirty days of assignment or termination.

5.7. Private Management Control Agreement. In order to access the CLETS/CORI systems, the Contractor shall sign the Private Management Control Agreement (Exhibit 12.1.1-4).

5.8. Security Addendum. The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Addendum (Exhibit 12.1.1-5) shall be signed.

5.9. Compliance with Laws. All CORI/CLETS rules, regulations, policies, practices and procedures will be adhered to by all parties involved, at all times. Contractor's failure to comply with any applicable laws and regulations is considered a breach of security and may result in the termination for default of the Agreement.

6. PERSONNEL ACCESS

6.1. In addition to the other background requirements set forth in this Schedule 12.1.1, it is the "County's policy to require that all permanent, temporary and seasonal employees, contractors and volunteers be issued and display a County ID card while on duty and/or within County facilities". Therefore, Contractor personnel performing Services at a Location shall comply with (i) County Administration Manual 0040-06 County Identification / Access Card Program and (ii) Department of General Service Policy and Procedure – Facilities Section entitled 3.1.6 SECURITY, as described in Section 12.1.3 of the Agreement.

6.2. Background Investigation

6.2.1. Background Investigations

Background investigations on Contractor personnel shall be conducted in accordance with the Standards and Procedures Manual and the Department of General - Services Policy & Procedures sections entitled 3.1.6.1 SECURITY CARD ACCESS SYSTEM and 3.1.6.4 CONTRACT SERVICE PROVIDER SECURITY REQUIREMENTS.

All Contractor personnel requiring access to any IT and telecommunications system supporting the delivery of the Services shall have passed an employee background investigation that is equivalent to that of the County. If the Contractor's employee background investigation policy, processes and procedures does not meet County standards, then the Contractor may use the County's background investigation process to fulfill this requirement.

6.2.2. County's Notification to Contractor

Contractor will be notified in the event that any Contractor personnel do not pass the background investigation. The County will not provide reasons or comments justifying such decision. However, should Contractor believe that there has been a mistake, then Contractor may bring the matter to the attention of the CIO.

6.2.3. County Issued I.D. Cards

6.2.3.1. After each Contractor personnel has successfully passed background investigation, the County will issue a County identification card (County ID card). The County ID card identifies Contractor personnel as being authorized to enter County facilities for the performance of Services and must be worn at all times during the performance of Services within any of the County's facilities.

6.2.3.2. County I.D. cards are for the exclusive use of the individual named and pictured on the card. Such cards shall remain the property of the County and shall be returned upon demand, or upon the termination or resignation of the individual, or upon termination or expiration of the Agreement.

6.2.3.3. Contractor shall assume all responsibility for all Contractor personnel's use of and the return of the County I.D. cards. Contractor shall be assessed one hundred (100) dollars (or such other fee as may be set forth in the Standards and Procedures Manual) for each County I.D. card not returned to the County. At the expiration and or termination of the Agreement, all or a portion of final payment may, at County's sole discretion, be withheld until all cards are accounted for.

6.2.4. Keys for County Facilities

6.2.4.1. Contractor may be temporarily issued a set of keys for County facilities that do not have guards on duty. Contractor shall assume all responsibilities for the use and prompt return of the keys. Any Contractor personnel holding keys to the County facilities shall use such keys solely to gain access to perform Services.

6.2.4.2. Keys issued to Contractor shall remain the property of the County and shall be returned upon demand or upon the termination or expiration of the Agreement. In addition to any other costs or damages, Contractor shall be assessed one hundred (100) dollars (or such other fee as may be set forth in the Standards and Procedures Manual) for each key not returned and will be further assessed the actual cost for parts and locksmith services to remove the lost key from the facility keying system(s).

6.2.4.3. If any key or access control card (County I.D. card) is lost or stolen, Contractor shall immediately notify the CIO in writing with the following information: the facility for which key(s) was lost, who lost the key(s), where the key(s) was lost, and the date / time loss was discovered.

6.2.4.4. Unauthorized duplication of keys to County facilities is a misdemeanor under Chapter 3, Section 469 of the California, Standard Penal Code.

6.2.5. Alarm Systems

6.2.5.1. The County has alarm systems in numerous facilities. In some instances there are multiple alarm systems within a facility. Contractor may be issued alarm codes and be instructed to properly operate the alarm systems. Contractor shall ensure that any Contractor personnel operating the alarm system be fluent in English. Failure to operate the alarm system correctly will result in a false alarm. Contractor will be responsible for all costs associated with false alarms.

6.2.5.2. In the event of a life threatening emergency, Contractor will instruct its personnel to use the standard operating procedures for emergency response, i.e. to call 911.

7. MISCELLANEOUS

7.1. Disclaimer. County makes no guarantee that compliance with this Agreement will be satisfactory for the Contractor's own purposes.

7.2. Amendment. The Parties agree to take action as necessary to amend this Schedule 12.1.1 from time-to-time as is necessary for County to comply with the requirements of any and all applicable other federal or State laws and regulations.

7.3. Judicial or Admin Proceedings. Contractor will notify County if it is named as a defendant in any criminal, civil, or administrative proceeding for a violation of any applicable security or privacy law.

7.4. Assistance in Litigation or Admin Proceedings. Contractor shall make itself and any of its agents available, at no cost to County, to testify, or otherwise, in the event of litigation or administrative proceedings commenced against County, its directors, officers, or employees, based on claimed violations of any applicable confidentiality, privacy, or security law or regulation, whether federal or State, if that litigation or proceeding involves actions of Contractor or its agents, except those where Contractor or its agents are named as an adverse party.

7.5. Interpretation. Any ambiguity in this Schedule 12.1.1 shall be resolved in favor of a meaning that permits County to comply with the applicable federal or State law or regulation.

7.6. Conflict. If a conflict between any of the standards contained in any of these enumerated sources of standards is found, Contractor shall follow the most stringent standard. The most stringent standard means that safeguard which provides the highest level of protection to County PHI and/or County PII/PI from unauthorized disclosure.

7.7. Regulatory References. All references in this Schedule 12.1.1 to any regulation or law mean the regulation or law currently in effect, including those legal and regulatory changes that occur after the effective date of this Agreement.

7.8. Survival. The respective rights and obligations of County and Contractor under this Schedule 12.1.1 shall survive the termination of the Agreement.

7.9. No Waiver of Obligations. No change, waiver, or discharge of any liability or obligation hereunder or any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, an any other occasion.

7.10. Due Diligence. Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Schedule 12.1.1 and is in compliance with all applicable federal and State laws and regulations, and that its agents, subcontractors, and vendors are in compliance with their obligations as required by this Schedule 12.1.1.

7.11. Effect of Termination. Upon termination of the Contract, for any reason, with respect to any and all County PHI and/or County PII/PI received from County, or created or received by Contractor on behalf of County:

7.11.1. Contractor shall return or destroy all County PHI and/or County PII/PI and retain no copies of County PHI and/or County PII/PI, except County PHI and/or County PII/PI necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities, as mutually agreed upon by the Parties.

7.11.2. Upon mutual agreement of the Parties that return or destruction of County PHI and/or County PII/PI is infeasible, Contractor shall extend the protections of this Schedule to such County PHI and/or County PII/PI for so long as Contractor maintains such County PHI and/or County PII/PI.

7.11.3. Contractor shall return to County or destroy, as determined by County, County PHI and/or County PII/PI retained by Contractor when it is no longer needed by Contractor for its proper management and administration or to carry out its legal responsibilities.

7.11.4. This provision shall apply to County PHI and/or County PII/PI that is in the possession of subcontractors or agents of Contractor.

END OF SCHEDULE