# MEMORANDUM OF UNDERSTANDING

BETWEEN [DEPARTMENT] (COVERED ENTITY)

AND [DEPARTMENT] (INTERNAL BUSINESS ASSOCIATE)

This Memorandum of Understanding (MOU) is entered into by and between the [DEPARTMENT] (hereinafter Covered Entity) and [DEPARTMENT] (hereinafter Internal Business Associate).

**RECITALS**

**WHEREAS,** CoveredEntity (CE) wishes to disclose certain information to Internal Business Associate (BA) for the purposes of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which may include Protected Health Information (PHI), to perform functions and/or services for or on behalf of the CE or as otherwise stated in this MOU; and

**WHEREAS**, both CE and BA are departments of San Bernardino County (County) and are included within the County’s designated Health Care Component; and

**WHEREAS**, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), as amended, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (HITECH Act), as amended, their implementing regulations, and other applicable laws; and

**WHEREAS**, The Privacy Rule and the Security Rule require CE to enter into an arrangement containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45 of the Code of Federal Regulations (C.F.R.), sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) and contained in this MOU; and

**WHEREAS**, Pursuant to HIPAA and the HITECH Act, BA must fulfill the responsibilities of this MOU by being in compliance with the applicable provisions of the HIPAA Standards for Privacy and Security of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), 164.400, 164.530 and 42 United States Code (U.S.C.) section 17932 (Breach Notification Rule), in the same manner as they apply to CE under HIPAA;

**NOW THEREFORE**, in consideration of the mutual promises below and the exchange of information pursuant to this MOU, the parties agree as follows:

1. **Definitions**

Unless otherwise specified herein, capitalized terms used in this MOU shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.

1. **Obligations and Activities of BA**
	1. Permitted Uses and Disclosures
		1. CE will Disclose PHI to BA only for the following purposes: [set forth details as to purpose of the BAA and what information will be shared, and for what purpose.]
		2. BA may Disclose PHI (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. If required by law and/or regulatory requirement, BA must obtain a written authorization from the Individual prior to making any other disclosures.
		3. If BA wishes to Disclose PHI to a third party for purposes not stated in this MOU, BA must obtain, prior to making any such Disclosure, (i) written authorization from an authorized representative of the CE for such disclosures; (ii) if authorization is given, reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this MOU and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (iii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. § 17932; 45 C.F.R. §§ 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]
	2. Prohibited Uses and Disclosures
		1. BA must not use, access or further disclose PHI other than as permitted or required by this MOU or as required by law. Further, BA must not use PHI in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. BA must disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder, except where otherwise permitted by law.
		2. BA must not use or disclose PHI for fundraising or marketing purposes.
		3. BA must not disclose PHI to a Health Plan for payment or Health Care Operations purposes if the patient has requested a special restriction, and/or has paid out of pocket in full for the health care item or service to which the PHI solely relates. (42 U.S.C. § 17935(a) and 45 C.F.R. § 164.522(a)(1)(i)(A).)
		4. BA must not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. § 17935(d)(2); and 45 C.F.R. § 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this Agreement.
	3. Appropriate Safeguards
2. BA must implement mutually acceptable safeguards in alignment with applicable laws and regulatory regulations to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. §§ 164.504(e)(2)(ii)(b) and 164.308(b).]
	1. *Cloud Storage* – Whenever possible, ePHI should be stored on secure network storage that is maintained by the County. EPHI that must be stored in the cloud must meet the requirements of Attachment A and must be approved by the CE and the County’s Innovation and Technology Department’s (ITD) Chief Information Security Officer (CSO).
	2. *Encryption*
		1. BA must not store any ePHI obtained from CE on any unencrypted portable media, hard drive, laptop, or tablet.
		2. EPHI must be encrypted when transmitted outside of the County network.
		3. Encryption must be 128 bit AES encryption or greater with separately stored decryption keys.
	3. *Anti-Virus/Anti-Malware -* BA must ensure that all workstations, laptops and other systems that process and/or store ePHI have a commercial third-party anti-virus/anti-malware software solution and are updated when a new anti-virus/anti-malware definition/software release is available.
	4. *Security Patches* - BA must ensure that all workstations, laptops and other systems that process and/or store ePHI have current security patches applied and are up-to-date.
	5. *Minimum Necessary* – BA must document and enforce physical and technical safeguards that ensure access by its workforce to CE’s PHI is restricted to the minimum necessary CE PHI required to fulfill the obligations of this MOU*.*
	6. *Restricted Access –* BA must restrict access to all areas where PHI is accessed, processed, maintained or stored to ensure that PHI and systems containing ePHI are protected from inappropriate access, use, disclosure, theft or loss.
3. In accordance with 45 C.F.R. section 164.316, BA must maintain current, reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule. These policies and procedures should be made available within a reasonable timeframe to the CE upon request.
4. BA must provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the CE’s PHI. These trainings and/or evidence of completion of such trainings should be made available to the CE within a reasonable timeframe upon request.

The training must include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the BA under this MOU.

* 1. Assessments

BA must perform initial and ongoing assessments to review the written policies and procedures for handling secured and confidential materials, and identify any policies or procedures that are either sources of data security weaknesses or barriers to information sharing. BA must review any history of data security breaches or near-breaches, and lessons learned.

* 1. Electronic Security Protections Review

BA must review electronic security protections and methods of electronic data transfer and storage to ensure they comply with the requirements of this MOU and are sufficient to protect shared PHI.

* 1. County Policy

BA must adhere to the County Policy Manual, including but not limited to Chapter 14, as well as other CE-specific policies and procedures.

* 1. Subcontractors

BA must enter into written agreements with agents and subcontractors to whom BA provides CE’s PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this MOU.

* 1. Reporting of Improper Access, Use or Disclosure or Breach

Every suspected and actual Breach must be reported immediately, but no later than one (1) business day upon discovery, to CE’s Office of Compliance and ITD’s CISO, consistent with the regulations under HITECH Act. Upon notification from BA, CE will coordinate notification of the actual or suspected Breach to the County HIPAA Privacy Officer. Upon discovery of a Breach or suspected Breach, BA must complete the following actions:

* + 1. Provide CE’s Office of Compliance and ITD’s CISO with the following information to include but not limited to:
			1. Date the Breach or suspected Breach occurred;
			2. Date the Breach or suspected Breach was discovered;
			3. Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;
			4. Number of potentially affected Individual(s) with contact information; and
			5. Description of how the Breach or suspected Breach allegedly occurred.
		2. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:
			1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
			2. The unauthorized person who had access to the PHI;
			3. Whether the PHI was actually acquired or viewed; and
			4. The extent to which the risk to PHI has been mitigated.
		3. Provide a completed risk assessment and investigation documentation to CE’s Office of Compliance and ITD’s CISO within ten (10) calendar days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the discretion of CE, additional information may be requested.
			1. If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.
			2. If a Breach has occurred, notification to the Individual(s) is required and BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.
		4. Make available to CE and governing state and federal agencies in a time and manner designated by CE or governing state and federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the CE reserve the right to conduct its own investigation and analysis.
	1. Access to PHI

To the extent BA maintains a Designated Record Set on behalf of CE, BA must make PHI maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) calendar days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA must provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA must immediately forward such request to CE.

* 1. Amendment of PHI

If BA maintains a Designated Record Set on behalf of the CE, BA must make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE’s obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

* 1. Access to Records

BA must make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE’s compliance with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary must also be provided to the CE upon request.

* 1. Accounting for Disclosures

BA, its agents and subcontractors must document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of treatment, payment, and health care operations. BA must provide an accounting of disclosures to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained must include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the Individual’s authorization, or a copy of the written request for disclosure.

* 1. Termination

CE may immediately terminate this MOU, and any related agreements, if CE determines that BA has breached a material term of this MOU. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

* 1. Return of PHI

Upon termination of this MOU, BA must return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA must provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this MOU, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this MOU, and to limit any further use, access or disclosures.

* 1. Breach by the CE

Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE’s obligations under this MOU, the BA must take reasonable steps to address the Breach and/or end the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non-compliant activity, the BA must terminate the MOU (if feasible) and report the violation to the Secretary of HHS.

* 1. Mitigation

BA must have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to BA of a use, access or disclosure of PHI by BA, its agents or subcontractors in violation of the requirements of this MOU.

* 1. Costs Associated to Breach

BA shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the CE and shall not be reimbursable under the MOU at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

* + - Postage;
		- Alternative means of notice;
		- Media notification; and
		- Credit monitoring services.
	1. Direct Liability

BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA’s compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

* 1. Assistance in Litigation or Administrative Proceedings

BA must make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the MOU, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

* 1. *\*If applicable* BA Staff at CE Facilities/Locations

BA staff that are located on-site or are provided access to a CE facility or location must complete all training, policy review, and comply with CE policies and procedures at the discretion of the CE.

1. **Obligations of CE**
	1. CE shall notify BA of any of the following, to the extent that such may affect BA’s use, access, maintenance or disclosure of PHI:
		1. Any limitation(s) in CE’s notice of privacy practices in accordance with 45 C.F.R. section 164.520.
		2. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.
		3. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.
2. **General Provisions**
	1. Term

This MOU is effective as of the date fully executed and shall continue for a period of \_\_\_\_\_ years/months unless otherwise terminated earlier by the Parties.

* 1. Department Contact

CE and BA must identify a member of department management who must be responsible for implementation and enforcement of the requirements of this MOU. The identified member must have the authority to make decisions about operations that may affect authorizing, accessing, or using the data and should serve as the contact for inquiries regarding the security and confidentiality policies and practices.

* 1. Ownership

The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

* 1. Regulatory References

A reference in this MOU to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

* 1. Amendment

The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of this MOU may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this MOU when and as necessary to comply with applicable laws. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the MOU upon written notice. To the extent an amendment to this MOU is required by law and this MOU has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this MOU automatically and without further action required by either of the parties. Subject to the foregoing, this MOU may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

* 1. Interpretation

Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy Rule, Security Rule, the HITECH Act, and all applicable patient confidentiality regulations.

* 1. Compliance with State Law

In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. (“CMIA”)). If any provisions of this MOU or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then BA must comply with the more restrictive requirements.

* 1. Survival

The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient’s PHI shall survive the termination of this Agreement.

* 1. Dispute Resolution

CE and BA agree they will establish mutually satisfactory methods for problem resolution at the lowest possible level as the optimum, with a procedure to escalate problem resolution through the appropriate chain-of-command, as deemed necessary.

**E. Conclusion**

1. This MOU, consisting of eight (8) pages and Attachment A, is the full and complete document describing the parties’ responsibilities and obligations as it relates to the exchange of PHI between the parties under this MOU.
2. The signatures of the Parties affixed to this MOU affirm that they are duly authorized to commit and bind their respective departments to the terms and conditions set forth in this document.

**IN WITNESS WHEREOF**, the Covered Entity and Internal Business Associate have each caused this MOU to be subscribed by its respective duly authorized representative, on its behalf.

|  |  |
| --- | --- |
|  |  |
|  | By ► |
|  | Name:  |
|  | Title:  |
|  | Dated: |
|  |  |
|  | By ► |
|  | Name:  |
|  | Title:  |
|  | Dated: |

**ATTACHMENT A**

**CLOUD SERVICES TERMS AND CONDITIONS**

These Cloud Services Terms and Conditions are attached to, form a part of, and supplement the MOU between CE and BA only with respect to ePHI stored with cloud services.

1. **DEFINITIONS**

Capitalized terms used herein have the same meaning as ascribed in the MOU. In addition, the following capitalized terms shall have the meaning ascribed herein:

* 1. “CISO”: County Chief Information Security Officer or other County-designated officer responsible for cyber-infrastructure security.
	2. “Cloud Service”: Generally, SaaS, PaaS, and/or IaaS used to store ePHI.
	3. “CSP”: Cloud Service Provider is the contracted derivative or direct provider of Cloud Services.
	4. “CONUS”: Continental United States
	5. “County Data”: Any information, formulae, algorithms, or other content that County, County’s employees, agents and end users upload, create or modify using the SaaS pursuant to this Contract. County Data also includes user identification information, personally identifiable information, and metadata which may contain County Data or from which County Data may be ascertainable.
	6. “Data Breach”: Any access, destruction, loss, theft, use, modification or disclosure of County Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.
	7. “IaaS” (Infrastructure as a Service): Service Provider provides the underlying cloud infrastructure for processing, storage, networks, and other fundamental computing resources that the customer does not manage or control, but the customer has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
	8. “PaaS” (Platform as a Service): Applications running on a cloud infrastructure managed or controlled by the Service Provider that are client-created or acquired using programming languages and tools supported by the Service Provider, but deployed onto the cloud infrastructure and controlled by client.
	9. “Recovery Point Objective (RPO)”: The point in time at which County Data can be recovered and/or systems restored when service is restored after an interruption. The Recovery Point Objective is expressed as a length of time between the interruption and the most proximate backup of County Data immediately preceding the interruption. The RPO is detailed in the SLA.
	10. “Recovery Time Objective (RTO)”: The period of time within which information technology services, systems, applications and functions must be recovered following an unplanned interruption. The RTO is detailed in the SLA.
	11. “SaaS” (Software as a Service): Applications running on a cloud infrastructure managed or controlled by the Service Provider including network, servers, operating systems, or storage, that are accessed by client devices through a thin client interface such as a web browser.
	12. “Service Provider”: Contractor, as defined in the General Terms or the individual or entity that is the owner of the rights to the Software.
1. **CLOUD SERVICE AVAILABILITY**

The Cloud Service shall be available twenty-four (24) hours per day, 365/366 days per year. If Cloud Service monthly availability averages less than 99.99% (excluding agreed-upon maintenance downtime), County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SLA. If Cloud Service monthly availability averages less than 99.99% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, County may terminate the contract for material breach. Service Provider shall provide advance written notice to County of any major upgrades or changes that will affect the Cloud Service availability.

1. **DATA AVAILABILITY**

County Data shall be available twenty-four (24) hours per day, 365/366 days per year. If County Data monthly availability averages less than 99.99% (excluding agreed-upon maintenance downtime), County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SLA if County is unable to access County Data as a result of: (i) acts or omission of Service Provider; (ii) acts or omissions of third parties working on behalf of Service Provider; (iii) network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Service Provider’s server, to the extent such attack would have been prevented by Service Provider taking reasonable industry standard precautions; (iv) power outages or other telecommunications or Internet failures, to the extent such outages were within Service Provider’s direct or express control. If County Data monthly availability averages less than 99.99% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, County may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions – Information Technology.

1. **SaaS and SECURITY**
	1. **Certification**

Service Provider shall certify:

* + 1. the sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract, and, if requested by County, provide a copy of its Statement on Standards for Attestation Engagements (SSAE) 18 Service Organization Control (SOC) 2 Type II audit results;
		2. its compliance with the California Information Practices Act (Civil Code Sections 1798 et seq.);
		3. its compliance with privacy provisions of the Federal Privacy Act of 1974; and
		4. its compliance with applicable industry standards and guidelines, including but not limited to relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCI/DSS Cloud Computing Guidelines.
	1. **Safeguards**

Service Provider shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section D.1.a above at all times during the term of this Contract to secure County Data from Data Breach, protect County Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt and/or compromise County’s access to County Data.

* 1. **High-Availability and Redundancy**

Service Provider shall have a high-availability and a redundant environment, where the minimum requirements are:

* + 1. Power and/or generators shall be 2N
		2. UPS power shall be 2N
		3. Redundant servers shall be N+1
		4. Data center shall be Tier-2
		5. Data center cooling shall be 2N
		6. All UPS’s and Generators must be tested and inspected on a quarterly basis. Copies of inspection and testing results must be provided upon demand to the County. Inspection and testing records must be retained for a minimum of 3 years
		7. Data center cooling must have preventative maintenance performed quarterly. Copies of preventative maintenance records must be provided upon demand to the County. Preventative maintenance records must be retained for a minimum of 3 years.
	1. **Physical**

Service Provider shall have a reasonable physical security environment, where the minimum requirements are:

* + 1. Physical access to facility, data center(s), and/or server room(s) is restricted using an access control system that utilizes iCLASS SE or multiclass SE readers.
		2. Access control system must be capable of restricting access by time of day and groups
		3. Access control system must be auditable providing customize reports on demand for inspection by the County
		4. Access control system components and batteries must be inspected annually.
		5. Access control system batteries must be replaced every 3 years or when they fail
		6. Vendor must be able retain access control history for a minimum of 3 years or as required by law
		7. Alerts are generated when physical security has been breached by the access control system or intrusion detection system
		8. Intrusion detection systems must be monitored by a third party UL central station
		9. Intrusion detection systems must be inspected and tested quarterly with signals sent to the central station. Testing reports must be retained for 3 years and provided on demand by the County.
		10. Intrusion detection batteries must be inspected annually and replaced every 3 years or when they fail.
		11. Facility, data center(s), and server room(s) have an appropriate Video Surveillance System in-place for surveillance.
		12. Video surveillance system must have the capability to interface with the access control system and intrusion detection system
		13. Video surveillance system must be inspected quarterly to make sure cameras are recording and video is being archived
		14. Video surveillance system must archive video as per California Government Sections § 26202.6, § 34090.6 and § 53160
		15. All access control systems, intrusion detection systems and video surveillance systems must be on the facilities emergency power system and protected by UPS.
		16. Data center have protections in-place that minimize environmental issues such as temperature, fire, smoke, water, dust, electrical supply interference, and electromagnetic radiation.
		17. A chemical fire suppression system installed in the data center as per NFPA 2001.
		18. The chemical fire suppression system must be inspected semiannually as per NFPA 2001 §8.3
		19. Smoke detectors under the raised floors.
		20. Water detection system under the raised floors and above the ceiling.
		21. Facility must be protected 100% by an automatic fire sprinkler system with the data center being protected with an automatic pre-action fire sprinkler system.
		22. Facility automatic fire alarm system must be tested and inspected as per NFPA 25
	1. **Verification**

Service Provider shall provide a Statement on Standards for Attestation Engagements 16 (SSAE16) Service Organization Controls Report (SOC) 1 and SOC 2 Type I and Type II Reports on an annual basis. Based on the report(s), its findings and remediation planned or accomplished shall be provided to the County CISO in terms of an attestation letter. Service Provider shall also provide statistics specific to SaaS environment on a mutually agreed upon frequency with County that includes without limitation to performance, information security, network, and other pertinent SaaS data related to the Contract, at no cost to County.

* 1. **Security**

Service Provider assumes responsibility for the security and confidentiality, integrity, and availability of County Data under its control. No County Data shall be copied, modified, destroyed or deleted by Service Provider other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by CISO. When data is destroyed or disposed, it shall be in accordance with the National Institute of Standards of Technology (NIST) Special Publication 800-88 published by the U.S. Department of Commerce. The incorporation of the Defense of Department (DoD) standard 5220.2-M wipe method shall be used when using data destruction programs, file shredders, etc. In either case, a written confirmation of this process is required to the County CISO within three (3) days of the destroyed/disposed data. Remote access to County Data from outside the CONUS, including remote access to County Data by authorized SaaS support staff in identified support centers, is prohibited unless approved in advance by the CISO.

1. **ENCRYPTION**

In order to provide reasonable security to County Data, cloud service datacenters should encrypt all County Data while in route to and from the Service Provider (in motion) using secure transfer methods (e.g., Secure Sockets Layer, Transport Layer Security), and while stored in the datacenter (at rest)

* 1. **Data In Motion**

All transmitted County Data require encryption in accordance with:

* + 1. NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and
		2. NIST Special Publication 800-57 Recommendation for Key Management - Part 3: Application-Specific
		3. Key Management Guidance; and
		4. Secure Sockets Layer (SSL) is minimally required with minimum cipher strength of 128-bit.
	1. **Data At Rest**

All County Data at rest require encryption in accordance with:

* + 1. Federal Information Processing Standard Publication (FIPS) 140-2; and
		2. National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management - Part 1: General (Revision 3); and
		3. NIST Special Publication 800-57 Recommendation for Key Management - Part 2: Best Practices for
		4. Key Management Organization; and
		5. NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.
		6. Advanced Encryption Standard (AES) with cipher strength of 256-bit is minimally required.
1. **DATA LOCATION**

Unless otherwise stated in the Statement of Work and approved in advance by the CISO, the physical location of Service Provider’s data center where County Data is stored shall be within the CONUS, and County Data shall not be transmitted, processed or stored outside of CONUS

1. **RIGHTS TO DATA**

The parties agree that as between them, all rights, including all intellectual property rights, in and to County Data shall remain the exclusive property of County, and Service Provider has a limited, non-exclusive license to access and use County Data as provided to Service Provider solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to County Data, including user tracking and exception County Data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of County Data by Service Provider or third parties is prohibited. For the purposes of this requirement, the phrase “unauthorized use” means the data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized

1. **TRANSITION PERIOD**

For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall assist County in extracting and/or transitioning all County Data in the format determined by the County (“Transition Period”). The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment. During the Transition Period, SaaS and County Data access shall continue to be made available to County without alteration. Service Provider agrees to compensate County for damages or losses County incurs as a result of Service Provider’s failure to comply with this section. Unless otherwise stated in the SOW, the Service Provider shall permanently destroy or render inaccessible any portion of County Data in Service Provider’s and/or subcontractor’s possession or control following the expiration of all obligations in this section. Within thirty (30) days, Service Provider shall issue a written statement to County confirming the destruction or inaccessibility of County Data. County at its option, may purchase additional transition services as agreed upon in the SOW

1. **DATA BREACH**
	1. **Notification**

Upon discovery or reasonable belief of any Data Breach, Service Provider shall notify the CISO by the fastest means available and in writing to the County Notices contact within twenty-four (24) hours after Service Provider reasonably believes a Data Breach has occurred. At a minimum, the notification shall include:

* + 1. the nature of the Data Breach;
		2. County Data accessed, used or disclosed;
		3. any evidence of County Data extricated;
		4. the identity of the person(s) who accessed, used, disclosed and/or received County Data (if known);
		5. the law enforcement agency(ies) contacted; and
		6. actions taken or will be taken to quarantine and mitigate the Data Breach; and
		7. corrective action taken or will be taken to prevent future Data Breaches.
	1. **Investigation**

Service Provider shall conduct an investigation of the Data Breach and shall share the report of the investigation with the CISO. If required by law, County and/or its authorized agents shall have the right to lead or participate in the investigation, in its sole discretion. Service Provider shall cooperate fully with County, its agents and law enforcement.

* 1. **Post-Breach Audit**

Upon advance written request, Service Provider agrees that the County or its designated representative shall have access to Service Provider’s SaaS, operational documentation, records and databases, including online inspection, that relate to the SaaS that experienced the Data Breach. The online inspection shall allow the County, its authorized agents, or a mutually acceptable third-party to test that controls are in-place and working as intended. Tests may include, but not be limited to, the following:

* + 1. Operating system/network vulnerability scans,
		2. Web application vulnerability scans,
		3. Database application vulnerability scans, and
		4. Any other scans to be performed by the County or representatives on behalf of the County.
1. **DISASTER RECOVERY AND BUSINESS CONTINUITY**
	1. **Notification**

In the event of disaster or catastrophic failure that results in significant loss of County Data or access to County Data, Service Provider shall notify County by the fastest means available and in writing, with additional notification provided to the CISO. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contactor shall inform County of:

* + 1. the scale and quantity of County Data loss;
		2. Service Provider’s action plan to recover County Data and mitigate the results of County Data loss; and
		3. Service Provider’s corrective action plan to prevent future County Data loss.
	1. **Restore and Repair Service**

Service Provider shall:

* + 1. restore continuity of SaaS,
		2. restore County Data in accordance with the RPO and RTO as set forth in the SLA,
		3. restore accessibility of County Data, and
		4. repair SaaS as needed to meet the performance requirements stated in the SLA.
	1. **Investigation and Audit**

Service Provider shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with County. At its sole expense, Service Provider will have an independent, industry-recognized, County-approved third party perform an information security audit. Within five (5) business days of Service Provider’s receipt of the final report, Service Provider will provide the County with a copy of the report and a written remediation plan.

[END OF CLOUD SERVICES TERMS]