Exhibit 1

INSURANCE CONTRACTUAL REQUIREMENTS

EXHIBIT 1

INSURANCE CONTRACTUAL REQUIREMENTS

CONTACT For additional information about compliance with City Insurance and Bond requirements, contact the Office of the City Administrative Officer, Risk Management at (213) 978-RISK (7475) or go online at www.lacity.org/cao/risk. The City approved Bond Assistance Program is available for those contractors who are unable to obtain the City-required performance bonds. A City approved insurance program may be available as a low-cost alternative for contractors who are unable to obtain City-required insurance.

CONTRACTUAL REQUIREMENTS

CONTRACTOR AGREES THAT:

1. **Additional Insured/Loss Payee.** The CITY must be included as an Additional Insured in applicable liability policies to cover the CITY'S liability arising out of the acts or omissions of the named insured. The CITY is to be named as an Additional Named Insured and a Loss Payee As Its Interests May Appear in property insurance in which the CITY has an interest, e.g., as a lien holder.

2. **Notice of Cancellation.** All required insurance will be maintained in full force for the duration of its business with the CITY. By ordinance, all required insurance must provide at least thirty (30) days' prior written notice (ten (10) days for non-payment of premium) directly to the CITY if your insurance company elects to cancel or materially reduce coverage or limits prior to the policy expiration date, for any reason except impairment of an aggregate limit due to prior claims.

3. **Primary Coverage.** CONTRACTOR will provide coverage that is primary with respect to any insurance or self-insurance of the CITY. The CITY'S program shall be excess of this insurance and non-contributing.

4. **Modification of Coverage.** The CITY reserves the right at any time during the term of this Contract to change the amounts and types of insurance required hereunder by giving CONTRACTOR ninety (90) days' advance written notice of such change. If such change should result in substantial additional cost to CONTRACTOR, the CITY agrees to negotiate additional compensation proportional to the increased benefit to the CITY.

5. **Failure to Procure Insurance.** All required insurance must be submitted and approved by the Office of the City Administrative Officer, Risk Management prior to the inception of any operations by CONTRACTOR.

CONTRACTOR'S failure to procure or maintain required insurance or a self-insurance program during the entire term of this Contract shall constitute a material breach of this Contract under which the CITY may immediately suspend or terminate this Contract or, at its discretion, procure or renew such insurance to protect the CITY'S interests and pay any and all premiums in connection therewith and recover all monies so paid from CONTRACTOR.

6. **Workers' Compensation.** By signing this Contract, CONTRACTOR hereby certifies that it is aware of the provisions of Section 3700 *et seq.*, of the California Labor Code which require every employer to be insured against liability for Workers' Compensation or to undertake

self-insurance in accordance with the provisions of that Code, and that it will comply with such provisions at all time during the performance of the work pursuant to this Contract.

7. California Licensee. All insurance must be provided by an insurer admitted to do business in California or written through a California-licensed surplus lines broker or through an insurer otherwise acceptable to the CITY. Non-admitted coverage must contain a **Service of Suit** clause in which the underwriters agree to submit as necessary to the jurisdiction of a California court in the event of a coverage dispute. Service of process for this purpose must be allowed upon an agent in California designated by the insurer or upon the California Insurance Commissioner.

8. Aggregate Limits/Impairment. If any of the required insurance coverages contain annual aggregate limits, CONTRACTOR must give the CITY written notice of any pending claim or lawsuit which will materially diminish the aggregate within thirty (30) days of knowledge of same. You must take appropriate steps to restore the impaired aggregates or provide replacement insurance protection within thirty (30) days of knowledge of same. The CITY has the option to specify the minimum acceptable aggregate limit for each line of coverage required. No substantial reductions in scope of coverage which may affect the CITY'S protection are allowed without the CITY'S prior written consent.

9. Commencement of Work. For purposes of insurance coverage only, this Contract will be deemed to have been executed immediately upon any party hereto taking any steps that can be considered to be in furtherance of or towards performance of this Contract. The requirements in this Section supersede all other sections and provisions of this Contract, including, but not limited to, PSC-3, to the extent that any other section or provision conflicts with or impairs the provisions of this Section.

Required Insurance and Minimum Limits

Name: _____ Date: _____

Agreement/Reference: _____

Evidence of coverages checked below, with the specified minimum limits, must be submitted and approved prior to occupancy/start of operations. Amounts shown are Combined Single Limits ("CSLs"). For Automobile Liability, split limits may be substituted for a CSL if the total per occurrence equals or exceeds the CSL amount.

Limits

_____**Workers' Compensation (WC) and Employer's Liability (EL)**

WC *Statutory*
EL _____

☐ Waiver of Subrogation in favor of City

☐ Longshore & HarborWorkers
☐ Jones Act

_____ **General Liability** _____ _____

☐ Products/Completed Operations
☐ Fire Legal Liability _____
☐

☐
Sexual Misconduct _____

_____

_____ **Automobile Liability** (for any and all vehicles used for this contract, other than commuting to/from work) _____

_____ **Professional Liability** (Errors and Omissions) _____

Discovery Period _____

_____ **Property Insurance** (to cover replacement cost of building - as determined by insurancecompany) _____

☐ All Risk Coverage
☐ Flood _____
☐ Earthquake _____

☐ Boiler and Machinery
☐ Builder's Risk
☐ _____

_____ **Pollution Liability** _____

☐ _____

_____**Surety Bonds** - Performance and Payment (Labor and Materials) Bonds _____
_____**Crime Insurance** _____

Other: _____

_____

_____

(Rev. 05/18)

CITY OF LOS ANGELES

INSTRUCTIONS AND INFORMATION

ON COMPLYING WITH CITY INSURANCE REQUIREMENTS

(Share this information with your insurance agent or broker)

1. **Agreement/Reference** All evidence of insurance should identify the nature of your business with the CITY. Clearly show any assigned number of a bid, contract, lease, permit, etc. or give the project name and the job site or street address to ensure that your submission will be properly credited. Provide the **types of coverage and minimum dollar amounts** specified on the Required Insurance and Minimum Limits sheet (Form Gen. 146) included in your CITY documents.

2. **When to Submit** Normally, no work may begin until a CITY insurance certificate approval number ("CA number") has been obtained, so insurance documents should be submitted as early as practicable. For **As-needed Contracts**, insurance need not be submitted until a specific job has been awarded. **Design Professionals** coverage for new construction work may be submitted simultaneously with final plans and drawings, but before construction commences.

3. **Acceptable Evidence and Approval** Electronic submission is the required method of submitting your documents. **KwikComply** is the CITY's online insurance compliance system and is designed to make the experience of submitting and retrieving insurance information quick and easy. The system is designed to be used by insurance brokers and agents as they submit client insurance certificates directly to the City. It uses the standard insurance industry form known as the **ACORD 25 Certificate of Liability Insurance** in electronic format. **KwikComply** advantages include standardized, universally accepted forms, paperless approval transactions (24 hours, 7 days per week), and security checks and balances. The easiest and quickest way to obtain approval of your insurance is to have your insurance broker or agent access **KwikComply** at https://kwikcomply.org/ and follow the instructions to register and submit the appropriate proof of insurance on your behalf.

Contractor must provide City a thirty (30) day notice of cancellation (ten (10) days for nonpayment of premium) AND an Additional Insured Endorsement naming the CITY an additional insured completed by your insurance company or its designee. If the policy includes an automatic or blanket additional insured endorsement, the Certificate must state the CITY is an automatic or blanket additional insured. An endorsement naming the CITY an Additional Named Insured and Loss Payee as Its Interests May Appear is required on property policies. All evidence of insurance must be authorized by a person with authority to bind coverage, whether that is the authorized agent/broker or insurance underwriter.

Additional Insured Endorsements DO NOT apply to the following:

- Indication of compliance with statute, such as Workers' Compensation Law.
- Professional Liability insurance.

Verification of approved insurance and bonds may be obtained by checking **KwikComply**, the CITY's online insurance compliance system, at https://kwikcomply.org/.

4. **Renewal** When an existing policy is renewed, have your insurance broker or agent submit a new Acord 25 Certificate or edit the existing Acord 25 Certificate through KwikComply at https://kwikcomply.org/.

5. **Alternative Programs/Self-Insurance** Risk financing mechanisms such as Risk Retention Groups, Risk Purchasing Groups, off-shore carriers, captive insurance programs and self-insurance programs are subject to separate approval after the CITY has reviewed the relevant audited financial statements. To initiate a review of your program, you should complete the Applicant's Declaration of Self-Insurance form (http://cao.lacity.org/risk/InsuranceForms.htm) to the Office of the City Administrative Officer, Risk Management for consideration.

6. **General Liability** insurance covering your operations (and products, where applicable) is required whenever the CITY is at risk of third-party claims which may arise out of your work or your presence or special event on City premises. **Sexual Misconduct**

coverage is a required coverage when the work performed involves minors. **Fire Legal Liability** is required for persons occupying a portion of CITY premises. Information on two CITY insurance programs, the SPARTA program, an optional source of low-cost insurance which meets the most minimum requirements, and the Special Events Liability Insurance Program, which provides liability coverage for short-term special events on CITY premises or streets, is available at (www.2sparta.com), or by calling (800) 420-0555.

7. **Automobile Liability** insurance is required only when vehicles are used in performing the work of your Contract or when they are driven off-road on CITY premises; it is not required for simple commuting unless CITY is paying mileage. However, compliance with California law requiring auto liability insurance is a contractual requirement.

8. **Errors and Omissions** coverage will be specified on a project-by-project basis if you are working as a licensed or other professional. The length of the claims discovery period required will vary with the circumstances of the individual job.

9. **Workers' Compensation and Employer's Liability** insurance are not required for single-person contractors. However, under state law these coverages (or a copy of the state's Consent To Self Insure) must be provided if you have any employees at any time during the period of this contract. Contractors with no employees must complete a Request for Waiver of Workers' Compensation Insurance Requirement (http://cao.lacity.org/risk/InsuranceForms.htm). **A Waiver of Subrogation** on the coverage is required only for jobs where your employees are working on CITY premises under hazardous conditions, e.g., uneven terrain, scaffolding, caustic chemicals, toxic materials, power tools, etc. The Waiver of Subrogation waives the insurer's right to recover (from the CITY) any workers' compensation paid to an injured employee of the contractor.

10. **Property** Insurance is required for persons having exclusive use of premises or equipment owned or controlled by the CITY. **Builder's Risk/Course of Construction** is required during construction projects and should include building materials in transit and stored at the project site.

11. **Surety** coverage may be required to guarantee performance of work and payment to vendors and suppliers. A **Crime Policy** may be required to handle CITY funds or securities, and under certain other conditions. **Specialty coverages** may be needed for certain operations. For assistance in obtaining the CITY required bid, performance and payment surety bonds, please see the City of Los Angeles Contractor Development and Bond Assistance Program website address at http://cao.lacity.org/risk/BondAssistanceProgram.pdf or call (213) 258-3000 for more information.

12. **Cyber Liability & Privacy** coverage may be required to cover technology services or products for both liability and property losses that may result when a CITY contractor engages in various electronic activities, such as selling on the Internet or collecting data within its internal electronic network. Contractor's policies shall cover liability for a data breach in which the CITY employees' and/or CITY customers' confidential or personal information, such as but not limited to, Social Security or credit card information are exposed or stolen by a hacker or other criminal who has gained access to the CITY's or contractor's electronic network. The policies shall cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft. The policies are required to cover liability arising from website media content, as well as property exposures from: (a) business interruption, (b) data loss/destruction, (c) computer fraud, (d) funds transfer loss, and (e) cyber extortion.

Required Insurance and Minimum Limits

Date: 5/28/2026

Contractor/Vendor Name: Harris & Harris, Ltd.

Agreement/Reference: Delinquent Accounts Collection Services

Evidence of coverages checked below, with the specified minimum limits, must be submitted and approved prior to occupancy/start of operations/commencement of ANY work. The amounts shown are Combined Single Limits ("CSLs"). For Automobile Liability, split limits may be substituted for a CSL if the total per occurrence equals or exceeds the CSL amount.

Workers' Compensation (WC) and Employer's Liability (EL): Yes

Min. Limit of WC: Statutory

Min. Limit of EL: $1000000

Waiver of Subrogation in favor of the City: Yes

Longshore & Harbor Workers: No

Jones Act: No

WC and EL Other:

General Liability - City of Los Angeles MUST be a named additional insured**: Yes**

Min. Limit: $1000000

Products/Completed Operations: Yes

Sexual Misconduct: No

Fire Legal Liability: No

General Liability Other:

Automobile Liability (for any and all vehicles used for this contract, other than commuting to/from work)**: No**

Professional Liability (Errors and Omissions)**: Yes**

Min. Limit: $1000000

Discovery Period: 12 months after completion of work or date of termination

Professional Liability Other:

Property Insurance (to cover replacement cost of building - as determined by insurance company)**: No**

Pollution Liability: No

Surety Bonds - Performance and Payment (Labor and Materials) Bonds**: No**

Crime Insurance: Yes

Min. Limit: $1000000

Crime Insurance Other:

Cyber Liability: No

Other: **Insurance certificate(s) MUST be submitted on the City's KwikComply site: https://kwikcomply.org/ and be re-submitted throughout the entire contract term so all required insurance remains valid and not expired.

**No imposed automobile insurance-- contractor must comply with California automobile liability laws.

ATTACHMENT B

BUSINESS ASSOCIATE AGREEMENT
(HIPAA)

BUSINESS ASSOCIATE AGREEMENT
BETWEEN
THE CITY OF LOS ANGELES
AND
HARRIS & HARRIS, LTD.

This **Business Associate Agreement** (the "Agreement"), is made as of the 16th day of April, 2026, (the "Effective Date"), by and between Harris & Harris, Ltd., on behalf of itself and its subsidiaries and affiliates, (together "Business Associate" or "Business Associates") and the City of Los Angeles ("City"), by and through the Los Angeles Fire Department (the "Covered Entity") and collectively shall be known as the "Parties" in this Agreement. The Agreement is intended to satisfy the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy, security, and breach notification rules promulgated by the U.S. Department of Health and Human Services at 45 C.F.R. Parts 160, 162 and 164, and the Health Information Technology for Economic and Clinical Health Act (hereinafter referred to as "HITECH"), each as amended from time to time (and collectively hereinafter referred to as "HIPAA Rules"), and to ensure compliance with applicable state and local confidentiality and breach notification laws, including and without limitation California law, to the extent not preempted and more stringent than the HIPAA Rules as defined under 45 CFR 160.202.

RECITALS

WHEREAS, Business Associate will perform Services for and on behalf of the Covered Entity involving the processing of Protected Health Information as further described in Annex A (Description of Services) attached hereto and incorporated by reference into this Agreement;

WHEREAS, Covered Entity and Business Associate may have entered into a primary contract (the "Contract") under which Business Associate performs Services involving the creation, receipt, maintenance, or transmission of Protected Health Information on behalf of Covered Entity, or, where no such Contract exists, this Agreement shall govern those Services as a standalone Business Associate Agreement between the Parties;

WHEREAS, the Parties acknowledge that such Protected Health Information is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations at 45 C.F.R. Parts 160 and 164;

WHEREAS, HIPAA requires that Covered Entity obtain satisfactory assurances that Business Associate will appropriately safeguard Protected Health Information and comply with all applicable privacy, security, and breach notification requirements; and

WHEREAS, the Parties intend this Agreement to satisfy the written-contract requirements set forth in 45 C.F.R. §164.502(e) and §164.504(e), and to ensure that

Business Associate provides the same level of protection of Protected Health Information as is required of Covered Entity under HIPAA and HITECH.

NOW THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the terms of the Agreement as follows:

A. DEFINITIONS.

Terms not otherwise defined herein shall have the meanings ascribed to them in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), its implementing regulations at 45 C.F.R. Parts 160 and 164, and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), as amended from time to time.

1. Administrative Data

"Administrative Data" means information created, received, or maintained for internal operational, logistical, or support purposes—such as system configurations, scheduling data, staffing records, budgeting materials, or internal communications—that is not used, in whole or in part, to make decisions about an individual and therefore does not form part of the Designated Record Set (DRS) as defined in 45 C.F.R. § 164.501, unless expressly identified otherwise in Annex B (Data Processing Activities). Nothing in this definition shall be construed to remove any information from the scope of Protected Health Information or Business Associate's obligations under this Agreement.

2. Breach

"Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under Subpart E of 45 C.F.R. Part 164, which compromises the security or privacy of such Protected Health Information, subject to the exceptions and exclusions in 45 C.F.R. § 164.402.

3. Business Associate

"Business Associate" or "BA" shall have the meaning given in 45 C.F.R. § 160.103 and refers to Harris & Harris, Ltd., its agents, and subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Covered Entity.

4. Contract

"Contract" means Los Angeles City Contract No. [*fill in the Contract ID*], if any, between the City of Los Angeles (City) and Harris & Harris, Ltd., acting as Business Associate, under which the Parties may agree to certain commercial or operational terms. The Contract is separate and distinct from this Agreement and does not modify or limit Business Associate's obligations under this Agreement with respect to Protected Health Information.

5. **Covered Entity (CE)**

"Covered Entity" or "CE" means the Los Angeles Fire Department, a Health Care Component (see "HCC") of the City of Los Angeles, which may operate as a Hybrid Entity as defined in 45 C.F.R. § 164.103 and as defined in this Agreement.

6. **Designated Record Set (DRS)**

"Designated Record Set" means a group of records maintained by or for Covered Entity that are:

(i) medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and

(iii) other records used, in whole or in part, by or for Covered Entity to make decisions about individuals, as defined in 45 C.F.R. § 164.501.

For purposes of this definition, "record" includes any item or grouping of information containing Protected Health Information that is maintained, collected, used, or disseminated by or for Covered Entity.

7. **De-Identified Information**

"De-Identified Information" means health information that has been de-identified in accordance with 45 C.F.R. § 164.502(d) and the standards and implementation specifications set forth in 45 C.F.R. § 164.514(a)–(b). All documentation supporting de-identification shall comply with the requirements in Section E.4 (De-Identified Information) and any additional specifications in Annex B (Data Processing Activities).

8. **Health Care Component (HCC)**

"Health Care Component" or "HCC" means those portions of a Hybrid Entity that perform covered functions under HIPAA. The LAFD has been designated as a Health Care Component of the City of Los Angeles pursuant to Los Angeles City Council actions (Council File No. 10-1181, July 30, 2010, as modified by Council File No. R3-0240, August 16, 2013).

9. **HIPAA**

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, including all amendments and implementing regulations at 45 C.F.R. Parts 160, 162, and 164.

10. HITECH Act ("HITECH")

"HITECH Act" or "HITECH" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, including all implementing regulations, guidance, and compliance dates.

11. Hybrid Entity

"Hybrid Entity" means, for purposes of this Agreement, the City of Los Angeles, a single legal municipal entity that performs both HIPAA-covered and non-covered functions and has designated certain components, including the LAFD, as Health Care Components in accordance with 45 C.F.R. § 164.103.

12. Individual

"Individual" means the person who is the subject of Protected Health Information, as defined in 45 C.F.R. § 160.103, and includes a Personal Representative authorized under 45 C.F.R. § 164.502(g).

13. Metadata

"Metadata" means information that describes, explains, or records the characteristics, structure, context, or management of other data, including but not limited to timestamps, audit trails, geolocation data, device identifiers, user credentials, or system-generated attributes.

Metadata may constitute Protected Health Information if it identifies or could reasonably be used to identify an individual or if it relates to an individual's past, present, or future physical or mental health condition, health care, or payment for care, consistent with 45 C.F.R. § 160.103.

Where metadata forms part of the Designated Record Set (DRS) or is otherwise linked to identifiable Protected Health Information, it shall be treated and safeguarded as Protected Health Information under this Agreement.

14. Protected Health Information ("PHI")

"Protected Health Information" or "PHI" has the meaning set forth in 45 C.F.R. § 160.103 and refers to individually identifiable health information transmitted or maintained in any form or medium by or on behalf of the Covered Entity.

15. Required by Law

"Required by Law" means a mandate contained in law that compels a use or disclosure of PHI consistent with 45 C.F.R. § 164.512(a).

16. **Security Incident**

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, including but not limited to breaches of unsecured Protected Health Information, as defined in 45 C.F.R. §164.304 and §164.402. Security Incident does not require include unsuccessful attempts such as pings, port scans, or unsuccessful log-in attempts. All reporting shall follow Annex C (Security Incident and Breach Information Annex).

17. **Secretary**

"Secretary" means the Secretary of the U.S. Department of Health and Human Services (HHS) or their authorized designee.

18. **Subcontractor**

"Subcontractor" means any person or entity to whom Business Associate delegates a function, activity, or Service involving the creation, receipt, maintenance, or transmission of PHI on behalf of Business Associate, as defined in 45 C.F.R. § 160.103.

19. **AI System**

"AI System" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. AI System-related data activities involving PHI are governed by Annex D (Artificial Intelligence ("AI") System and Automated Processing) Annex.

20. **Services**

"Services" means the activities, deliverables, and functions performed by Business Associates for and on behalf of Covered Entity that involve the creation, receipt, maintenance, processing, or transmission of Protected Health Information, as described in Annex A (Description of Services) and any related data-processing or support activities identified in Annex B (Data Processing Activities).

B. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION IN CONNECTION WITH SERVICES.

In connection with the Services provided by Business Associate to or on behalf of Covered Entity, as described in Annex A (Description of Services), Covered Entity may disclose to Business Associate certain Protected Health Information necessary for Business Associate to perform such Services. Business Associate shall use and disclose Protected Health Information solely for the purposes described in

Annex A and only as permitted by this Agreement, the HIPAA Privacy, Security, and Breach Notification Rules (45 C.F.R. Parts 160 and 164) and applicable law.

Business Associate shall comply with all applicable provisions of HIPAA, the HITECH Act, and their implementing regulations, as amended from time to time, including assuming all responsibilities and liabilities applicable to business associates under 45 C.F.R. Parts 160 and 164, for the duration of this Agreement.

C. RELATIONSHIP OF THE PARTIES; AGENCY.

The parties acknowledge and agree that Business Associate is an independent contractor and **not** an agent, partner, joint venture, or employee of the Covered Entity for purposes of state and municipal law. Nothing in this Agreement shall be construed to create any employment, agency, or fiduciary relationship between the Parties for purposes of state or federal law. Notwithstanding the foregoing, Business Associate recognizes that, exclusively for purposes of HIPAA Privacy and Security Rules and consistent with 45 C.F.R. §160.103 and §164.502(e)(1)(ii), Business Associate, its agents or subcontractors, may be considered to be acting "on behalf of" Covered Entity when performing functions or activities involving Protected Health Information which shall not be construed to alter their independent-contractor status. In such circumstances, Business Associate and its agents or subcontractors shall be subject to all HIPAA obligations and restrictions applicable to Covered Entity with respect to that Protected Health Information. Business Associate shall not represent itself as an agent of Covered Entity in any other context and shall have no authority to bind Covered Entity to any contract, covenant, or obligation except as expressly authorized in writing by Covered Entity. Business Associate shall remain fully responsible for the acts, omissions, and defaults of its agents or subcontractors to the same extent as if such acts or omissions were those of Business Associate itself.

D. RIGHTS AND OBLIGATIONS OF COVERED ENTITY.

1. Notice of Privacy Practices. Covered Entity shall notify Business Associate, in writing and without unreasonable delay, of any limitation in Covered Entity's Notice of Privacy Practices (45 C.F.R. §164.520) that may affect Business Associate's permitted uses or disclosures of Protected Health Information.

2. Individual Authorization. Covered Entity shall promptly inform Business Associate of any change in, or revocation of, an individual's authorization to use or disclose Protected Health Information, to the extent such change affects Business Associate's permitted activities.

3. Restriction on Use or Disclosure. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of Protected Health Information agreed to by Covered Entity under 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or

disclosure.

4. Permissible Requests. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would be impermissible under HIPAA, the HITECH Act, and their implementing regulations, including 45 C.F.R. §164.504(e)(2)(i).

5. Suspected or Confirmed Incident or Breach and Information Cooperation. Business Associate shall make the final determination as to whether any reported use or disclosure of Protected Health Information by Business Associate constitutes an incident or a suspected or confirmed breach of unsecured Protected Health Information within the meaning of 45 C.F.R. §164.402 and shall determine the need for notification under 45 C.F.R. §164.404, §164.406 and §164.408. Business Associate shall, upon Covered Entity's request, provide to Covered Entity all information utilized by Business Associate to make such determination, including, but not limited to:

   - a description of the incident, suspected or confirmed breach and the discovery timeline;
   - the categories and approximate volume of Protected Health Information involved;
   - mitigation and containment steps taken; and
   - copies of any forensic, investigative, or incident-response reports.

   All suspected or confirmed incident or breach details and supporting documentation shall be submitted in accordance with Annex C (Security Incident and Breach Information Annex), which is incorporated herein by reference and forms an integral part of this Agreement. Business Associate shall provide this information without unreasonable delay and in no event later than five (5) business days following Covered Entity's written request. Business Associate shall continue to supplement the information as new facts become known.

6. Covered Entity Rights. Covered Entity reserves the right to monitor Business Associate's compliance with this Agreement, to request evidence of safeguards, to audit relevant records, to require remediation of identified discrepancies, or to require additional documentation to support Covered Entity's analysis for regulatory reporting.

E. OBLIGATIONS OF BUSINESS ASSOCIATE.

Business Associate's obligations under this section are in addition to, and not in limitation of, Business Associate's notification under 45 C.F.R. §164.410 (Notification by a Business Associate).

Business Associate agrees to comply with applicable federal and state privacy and security laws, specifically the provisions of the HIPAA Administrative Simplification to the extent applicable to business associates. Business Associate shall ensure that these obligations are included in all downstream agreements in accordance with 45 C.F.R. 164.504(e)(2)(ii)(D).

1. Use and Disclosure of Protected Health Information.
Business Associate shall use or disclose Protected Health Information only as necessary to perform the Services described in Annex A (Description of Services), or as Required by Law, and only to the extent such use or disclosure is permitted by this Agreement and the HIPAA privacy and security rules (45 CFR Parts 160 and 164).

Business Associate shall not use or disclose Protected Health Information in any manner that would be impermissible if done by the Covered Entity, and shall implement appropriate administrative, physical, and technical safeguards to prevent such use or disclosure as required by 45 C.F.R. §164.504(e)(2)(ii)(B).

Without limiting the foregoing, Business Associate agrees that it shall not:

(a) Use Protected Health Information for marketing, product development, profiling, or any commercial purpose other than as authorized in writing by Covered Entity, in accordance with 45 C.F.R. §164.502(a)(5)(ii);

(b) Sell, externally disclose, put in secondary use, or de-identify, unless de-identification complies with §45 C.F.R. 164.514, Protected Health Information without express written authorization by Covered Entity's legal counsel or an administrative representative;

(c) Use Protected Health Information for machine learning, artificial intelligence training, algorithmic modeling, or similar automated processing activities or purposes except as expressly authorized in writing by Covered Entity's legal counsel or an administrative representative and in accordance with Annex D (Artificial Intelligence (System) and Automated Processing), which is incorporated herein by reference; and

(d) Disclose Protected Health Information to any third party other than as necessary to perform the Services under this Agreement (and as summarized in Annex A) and only after obtaining written assurances that such third party will (i) maintain confidentiality and security of Protected Health Information in accordance with this Agreement and the HIPAA Rules, and (ii) report to Business Associate, without unreasonable delay after discovery, any actual or suspected breach of unsecured Protected Health Information, unauthorized use or disclosure of Protected Health Information, or Security Incident so that Business Associate can meet its

own notification and mitigation obligations under the HIPAA Breach Notification Rules (45 C.F.R. §§164-400-414) and this Agreement.

(e) Use Protected Health Information for any a purpose other than its own proper management and administration of Protected Health Information or to carry out its legal responsibilities only to the extent permitted by 45 C.F.R. §164.504(e)(4), and only if Business Associate obtains reasonable assurances that any recipients will maintain Protected Health Information confidentially and notify Business Associate of any breach or violation as set forth in this Section.

2. Suspected or Confirmed Security Incident or Breach Notification.
(a) Prompt Notice of Impermissible Use or Disclosure. Business Associate shall report to the Covered Entity any suspected or confirmed Security Incident or Breach of unsecured Protected Health Information without unreasonable delay and no later than seventy-two (72) hours after discovery, as defined in 45 C.F.R. §164.402.

Business Associate's report shall be submitted in accordance with Annex C (Security Incident and Breach Information Annex) and shall include, at a minimum, the information described therein. Business Associate shall supplement its report promptly as additional facts become known and shall cooperate fully with Covered Entity's investigation and mitigation activities. Covered Entity retains sole authority to determine whether any incident constitutes a reportable breach under 45 C.F.R. §164.402, applying the four-factor risk assessment criteria in §164.402(2)(i)-(iv), and whether notification under §164.404-410 are required.

(b) Cooperation and Determination Breach. Business Associate acknowledges that Covered Entity is solely responsible for determining whether a reportable "breach" of unsecured Protected Health Information has occurred within the meaning of 45 C.F.R. §164.402 and for performing all required notifications under §§164.404, 164.406, and 164.408. Business Associate shall cooperate fully with Covered Entity's investigation, provide requested documentation, and implement reasonable mitigation measures at Business Associate's sole cost.

(c) Compliance with 45 C.F.R. §164.410 – Notification by a business associate. Business Associate shall comply with the breach-notification obligations applicable to business associates under 45 C.F.R. §164.410, including providing notification of a discovered breach no later than sixty (60) calendar days and maintaining written policies and records of all breach-related activities for at least six (6) years as required by §164.530(j)(2). Nothing in this subsection shall be interpreted to require Business Associate to provide notice directly to individuals or regulators unless Covered Entity directs otherwise in writing.

(d) Relationship Reminder. Business Associate performs the Services as an independent contractor to Covered Entity. The Parties' relationship is governed by Section C "Relationship of the Parties; Agency" clause. This paragraph is included for reference only and does not alter that relationship.

3. Data Aggregation.

(a) Limitation on Use.

Business Associate shall not use or disclose Protected Health Information for data aggregation, analytics, benchmarking, or any other combined-dataset activity involving Protected Health Information received from multiple Covered Entities, unless expressly authorized in advance and in writing by Covered Entity in accordance with 45 C.F.R. § 164.504(e)(2)(i)(B).

(b) Authorized Aggregation.

If Covered Entity provides written authorization for data aggregation, such use shall be limited exclusively to health-care operations, payment, or quality-improvement activities permitted under 45 C.F.R. § 164.506(c) and § 164.501, and shall remain subject to all applicable restrictions of this Agreement, including data-minimization, role-based access, and safeguard requirements under 45 C.F.R. §§ 164.308, 164.310, and 164.312.

(c) Prohibition on Secondary Use.

Business Associate shall not:

1. Combine or compare Covered Entity's Protected Health Information with Protected Health Information received from any other Covered Entity or client for marketing, product development, AI training, or other non-authorized purposes;
2. De-identify Covered Entity's Protected Health Information for independent commercial use under 45 C.F.R. § 164.514(b) without Covered Entity's prior written consent; or
3. Claim, assert or acquire any ownership, license, proprietary, or derivative rights in any aggregated or De-Identified Information created from or derived from Covered Entity's Protected Health Information, nor shall Business Associate use such information for any secondary, commercial, analytical, or model development purpose not covered in this Section and without Covered Entity's prior written authorization.

(d) Safeguards and Reporting.

Business Associate shall maintain logical segregation of Protected Health Information ("PHI") received from each Covered Entity and shall implement appropriate technical and administrative safeguards designed to prevent unauthorized access, use, disclosure, aggregation, analysis, or commingling of such PHI across Covered Entities. Such safeguards may include access controls, data partitioning, encryption, and monitoring controls, and shall not require physical segregation of systems or infrastructure. Business Associate shall promptly notify Covered Entity, without unreasonable delay and in accordance with this Agreement, upon discovery of any unauthorized aggregation, analysis, or commingling of Covered Entity's PHI.(e) Ownership and Control.

All Protected Health Information, whether individually or as part of an aggregated dataset, remains the sole property and in control of Covered Entity. Business Associate acquires no rights in Protected Health Information other than those necessary to perform Services and for duration of term of this Agreement. Any aggregated information created under Covered Entity's written authorization shall be deemed Covered Entity's confidential information and subject to the same protections as Protected Health Information under this Agreement.

4. De-identified Information.

(a) Business Associate may create, use, or disclose de-identified health information only if:

1. Written Authorization. Such use or disclosure is fully disclosed to and expressly authorized in writing by the Covered Entity, which may grant or withhold authorization in its sole discretion;
2. Regulatory Compliance. The de-identification is performed in strict compliance with 45 C.F.R. § 164.502(d) and meets the standards and implementation specifications for de-identification under 45 C.F.R. § 164.514(a) and (b); and
3. Methodology Disclosure. Business Associate shall document the de-identification process used, including whether the Expert Determination or Safe Harbor method was applied, and shall provide Covered Entity with a written summary of the techniques, tools, or statistical methods used to achieve de-identification, as required under § 164.514(b).
4. Limitations on Use. Business Associate shall not use or disclose any de-identified information for secondary or commercial purposes (including data analytics, AI model training, or research) without Covered Entity's prior written approval and shall not attempt or permit any re-identification of such information.

5. Safeguards. Business Associate shall maintain appropriate safeguards to ensure that Protected Health Information is not used or disclosed other than as permitted by this Agreement or as Required by Law. Business Associate shall implement the administrative, physical, and technical safeguards required by 45 C.F.R. §§ 164.308, 164.310, and 164.312, as applicable, to reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI ("ePHI") that it creates, receives, maintains, or transmits on behalf of Covered Entity.

   Such safeguards shall include, at a minimum:

   - Encryption of ePHI at rest and in transit consistent with NIST FIPS 140-2 validated cryptographic standards;
   - Maintenance of written policies and procedures for access control, audit logging, user authentication, and system monitoring; and
   - Integration of incident response and breach notification coordination with Covered Entity in accordance with Section E.13 (Incident Response).

   Business Associate shall, on an annual basis or upon reasonable request, provide Covered Entity with (i) a copy or executive summary of its most recent security risk analysis conducted pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A), and (ii) its corresponding risk management or remediation plan addressing identified vulnerabilities.

6. Minimum Necessary.

   Business Associate shall ensure that all uses, disclosures, and requests for Protected Health Information are limited to the minimum necessary to accomplish the intended purpose, in accordance with 45 C.F.R. § 164.514(d).

   To operationalize this requirement, Business Associate shall:

   - Implement role-based access controls (RBAC) limiting access to Protected Health Information solely to personnel whose job functions require such access, as documented in written access control matrices;
   - Establish tiered access permissions that differentiate between classes of users (e.g., billing, customer support, technical operations) to prevent overexposure of Protected Health Information;
   - Periodically review and validate user access rights (at least annually or upon role changes) to ensure compliance with the minimum necessary standard; and
   - Configure systems to limit query, view, and export functions to the minimum data elements necessary for each authorized task or transaction.

Business Associate shall document and make available to Covered Entity, upon reasonable request, its policies and procedures demonstrating adherence to this principle and the technical and administrative controls used to enforce it.

7. Disclosure to Agents and Subcontractors.

If Business Associate discloses Protected Health Information to any agent or subcontractor, Business Associate shall require that such agent or subcontractor agree in writing to the same restrictions, conditions, and safeguards that apply to Business Associate under this Agreement and in compliance with 45 C.F.R. § 164.502(e) and § 164.308(b).

Business Associate shall:

- Disclose in writing to Covered Entity all subcontractors that will create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate;
- Maintain and, upon request, provide Covered Entity with a current list of all subcontractors or agents that handle Protected Health Information;
- Ensure each subcontractor implements reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of Protected Health Information; and
- Make such subcontractors available for audit or inspection by Covered Entity upon reasonable notice.

Business Associate shall remain fully liable for any acts, omissions, or failures of its agents or subcontractors as if they were Business Associate's own.

8. Individual Rights Regarding Designated Record Sets.

If Business Associate maintains a Designated Record Set on behalf of Covered Entity, it shall support Covered Entity in fulfilling individuals' rights of access under 45 C.F.R. § 164.524 as follows:

(a) Access and Copies of Protected Health Information.

If Business Associate receives a direct request from an individual for access to or a copy of their Protected Health Information, Business Associate shall forward such request to Covered Entity within ten (10) calendar days of receipt to allow Covered Entity to comply with the 30-day response period under 45 C.F.R. § 164.524(b)(2).

Business Associate shall promptly assist Covered Entity in providing access in the requested form or format, if readily producible, or in an

agreed-upon summary format, and shall provide all relevant Protected Health Information necessary for Covered Entity's timely response.

Any reasonable, cost-based fees shall be administered in accordance with Covered Entity's established HIPAA policies.

(b) Amendment of Protected Health Information.

If Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate shall make such records available to Covered Entity for amendment in accordance with 45 C.F.R. § 164.526.

Upon receipt of a request for amendment, Business Associate shall notify Covered Entity within ten (10) calendar days and implement any approved amendment or link to the amendment statement as directed by Covered Entity.

(c) Accounting of Disclosures.

Business Associate shall maintain documentation of disclosures of Protected Health Information sufficient to enable Covered Entity to provide an accounting of disclosures under 45 C.F.R. § 164.528, including the date, purpose, and recipient of each disclosure not otherwise exempt.

Business Associate shall provide such documentation to Covered Entity within ten (10) calendar days of Covered Entity's request to allow Covered Entity to meet the 60-day response period required by the HIPAA Rule.

The accounting shall cover disclosures made in the six (6) years preceding the request (excluding those prior to the HIPAA compliance date).

The first accounting requested by an individual within any twelve-month period shall be provided at no cost; subsequent requests may incur a reasonable, cost-based fee, provided Covered Entity is notified in advance and given an opportunity to withdraw or modify the request.

(d) Cooperation and Documentation.

Business Associate shall maintain and make available to Covered Entity, upon request, all policies, logs, and procedures used to comply with this Section 8 and shall cooperate fully to ensure Covered Entity's timely and compliant response to individual rights requests.

9. Internal Practices, Policies and Procedures. Except as otherwise specified herein, Business Associate shall make available its internal practices,

policies and procedures relating to the use and disclosure of Protected Health Information, received from or on behalf of Covered Entity to the Secretary or his or her agents for the purpose of determining Covered Entity's compliance with the HIPAA Rules, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by Covered Entity or the Secretary.

10. Notice of Privacy Practices. Business Associate shall comply with the limitations set forth in Covered Entity's current Notice of Privacy Practices ("NPP"). Any changes to the NPP that affect Business Associate's permitted uses or disclosures of Protected Health Information shall apply only after Business Associate receives written notice of such changes. Uses or disclosures made in good-faith reliance on a prior NPP before receipt of the amended notice shall not constitute a breach of this Agreement.

11. Withdrawal of Authorization. If Business Associate's use or disclosure of Protected Health Information is based on an Individual's authorization and Business Associate receives notice that such authorization has been revoked, has expired, or is otherwise invalid, Business Associate shall immediately cease all use and disclosure of the affected Protected Health Information, except to the extent such actions were taken in good-faith reliance on a valid authorization prior to notice, or where an express HIPAA exception applies.

12. Knowledge of HIPAA Rules. Business Associate agrees to review and understand the HIPAA Rules as it applies to Business Associate, and to comply with the applicable requirements of the HIPAA Rule, as well as any applicable amendments.

13. Security Incident.

(a) Definition and Distinction.

For purposes of this Agreement:

- A "Security Incident" has the meaning set forth in 45 C.F.R. § 164.304 — the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations, involving electronic Protected Health Information.
- A "Breach" has the meaning set forth in 45 C.F.R. § 164.402, as reflected in the Definitions section of this Agreement, and triggers the notification obligations under 45 C.F.R. § 164.410.

(b) Incident Response Procedures.

Business Associate shall maintain and follow written incident detection, response, and documentation procedures designed to identify, contain, and remediate Security Incidents involving Protected Health Information or ePHI.

(c) Reporting Obligations.

1. Business Associate shall report any suspected or confirmed Security Incident to Covered Entity without unreasonable delay and no later than twenty-four (72) hours after discovery.
2. The initial notice shall include, to the extent known:

   (i) the nature and scope of the incident;

   (ii) the date and time of discovery;

   (iii) systems and data elements involved;

   (iv) estimated volume of records affected;

   (v) containment and mitigation measures taken; and

   (vi) contact information for Business Associate's incident lead.

3. Business Associate shall provide a follow-up written report within five (5) business days containing a root cause analysis, corrective action plan, and evidence of containment and recovery activities.

(d) Cooperation and Preservation.

Business Associate shall:

- Cooperate fully with Covered Entity, its designees, and law enforcement in any investigation or mitigation efforts;
- Preserve all relevant logs, records, and evidence for a minimum of six (6) years from the date of discovery; and
- Refrain from making public statements regarding the incident without Covered Entity's prior written approval.

(e) Breach Notification.

If Business Associate determines that a Security Incident constitutes a Breach of Unsecured Protected Health Information under 45 C.F.R. § 164.410, Business Associate shall provide Covered Entity with a written breach notification meeting the content and timing requirements of the HIPAA Breach Notification Rule.

(f) Continuous Improvement.

Following any incident or breach, Business Associate shall update its incident response plan and implement appropriate corrective and preventive measures to reduce the likelihood of recurrence and shall provide Covered Entity with documentation of such actions upon request.

F. TERM AND TERMINATION

1. Term. The Term of this Agreement shall be effective as of the Effective Date of the Contract, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

2. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(a) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(b) Immediately terminate this Agreement and the Contract if Business Associate has breached a material term of this Agreement and cure is not possible; or

(c) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

3. Effect of Termination.

(a) Return or Destruction of Protected Health Information.

Upon termination or expiration of this Agreement, for any reason, Business Associate shall immediately cease all use and disclosure of Protected Health Information received from, or created or maintained on behalf of, Covered Entity. Unless otherwise agreed based on technical feasibility, Business Associate shall, within thirty (30) days, return or securely destroy all such Protected Health Information, including all copies, extracts, or derivative data, in any form or medium, whether maintained by Business Associate or any of its agents or subcontractors.

Business Associate shall confirm completion of return or destruction to Covered Entity in writing, specifying:

- The date and method of destruction or return;
- The type and volume of Protected Health Information destroyed or returned; and
- The authorized individual who supervised the process.

No copies of Protected Health Information shall be retained by Business Associate, its agents or subcontractors, except as expressly provided in subsection (b).

(b) Infeasibility of Return or Destruction.

If Business Associate determines that return or destruction of Protected Health Information is infeasible, Business Associate shall, within ten (10) days of such determination, provide Covered Entity with written notice describing:

- The specific reasons why return or destruction is infeasible (e.g., legal retention obligations, backup dependencies, active litigation holds); and
- The approximate duration and scope of such infeasibility.

Upon Covered Entity's approval, Business Associate shall:

- Continue to safeguard the Protected Health Information in accordance with this Agreement and 45 C.F.R. Parts 160 and 164;
- Limit further use and disclosure to those purposes that make return or destruction infeasible; and
- Apply the same administrative, physical, and technical safeguards required under this Agreement until Protected Health Information is returned or destroyed.

(c) Bankruptcy and Cessation of Operations.

In the event Business Associate becomes insolvent, declares bankruptcy, ceases operations, or is otherwise unable to perform its obligations under this Agreement, Business Associate (or its lawful successor, trustee, or receiver) shall:

- Immediately notify Covered Entity of such event; and
- Return or securely destroy all Protected Health Information in its possession, custody, or control prior to or concurrent with cessation of operations.

No Protected Health Information may be treated as a bankruptcy estate asset, and title to all Protected Health Information remains vested exclusively in Covered Entity.

(d) Audit and Certification.

Upon Covered Entity's request, Business Associate shall certify in writing that it and its agents or subcontractors have complied with this Section, and Covered Entity may, at its discretion, audit or inspect Business Associate's destruction or return records to verify compliance.

Business Associate's obligations under this Section, including the duty to safeguard Protected Health Information and to limit its use and disclosure, shall survive termination of this Agreement for as long as Business Associate retains Protected Health Information.

G. LIABILITY, INDEMNIFICATION, MITIGATION, AND PROPRIETARY RIGHTS

1. Indemnification

(a) Regulatory Proceedings and Compliance Costs. For avoidance of doubt, the indemnification obligations under this Section expressly include all regulatory, administrative, and compliance-related costs that the Covered Entity reasonably incurs as a result of, or in connection with, any breach, Security Incident, or violation by Business Associates, its agents or subcontractor and excludes penalties to the extent not insurable or prohibited by law. Such indemnification amounts include, without limitation:

(i) Costs of responding to investigations, audits, inquiries, or enforcement actions by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), or any other federal or state authority;
(ii) Cost of implementing or monitoring any Corrective Action Plan (CAP), resolution agreement, or consent order imposed by OCR or any other regulatory body;
(iii) Attorneys' fees, expert, consulting, and forensic expenses incurred in responding to or defending such proceedings; and
(iv) Reasonable internal personnel costs and outside-vendor expenses associated with compliance reviews, risk analysis, documentation, and policy revisions that OCR or other regulatory require.

These costs are recoverable to the fullest extent permitted by 45 C.F.R. Part 160, Subpart D (Enforcement Rule) and applicable law, and are deemed first-party losses for purposes of indemnification and insurance coverage under this Agreement.

(b) To the extent permitted by law, Business Associate shall indemnify and hold harmless Covered Entity from and against all claims, demands, liabilities, losses, costs, fines, penalties, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, reasonable attorney's fees, defense costs, expert/forensic costs and equitable relief), for any damage or loss incurred by Covered Entity arising out of, resulting from, or attributable to:(i) Business Associate or its agent(s)/sub-contractor(s) breach of this Agreement; (ii) any violation of HIPAA, HITECH, or other applicable privacy or cybersecurity law by Business Associate, its agents or subcontractor; any security incident or breach of unsecured PROTECTED HEALTH INFORMATION (as defined in 45 CFR 164.402), attributable to acts or omissions of Business Associate, its agents/ or subcontractor; and (iv) any failure to comply with 45 CFR §§164.308-312 or §164.504(e). This indemnity shall not be construed to limit Covered Entity's rights, if any, to common law indemnity.

(c) First-Party Costs. Indemnified amounts include first-party costs reasonably incurred by the Covered Entity in responding to a Security Incident or Breach, including: investigation and forensics; containment and eradication; data restoration; legally required and Covered Entity-directed notifications; call-center services; credit monitoring/identity theft protection; mailing and printing; public relations/crisis communications; regulatory inquiries, audits, and OCR resolution/CAP implementation; and reasonable attorney's fees.

(d) Tender and Control of Defense. Upon written notice by Covered Entity of a claim subject to indemnity, Business Associate shall promptly assume the defense using counsel reasonably acceptable to Covered Entity. Covered Entity may participate at its own expense, provided however, if Covered Entity reasonably determines that a conflict of interest prevents joint representation, Business Associate shall fund separate counsel for Covered Entity that is reasonably acceptable to Business Associate. Business Associate shall not settle any claim without Covered Entity's prior written consent if the settlement: (1) imposes any non-monetary obligation on Covered Entity; (2) admits fault by Covered Entity; or (3) fails to unconditionally release Covered Entity. Covered Entity may elect to retain control of the defense with counsel of its choosing. In such event, Business Associate shall reimburse Covered Entity's reasonable defense costs for claims subject to indemnity.

(e) Subcontractor(s) and Agent(s) of Business Associate. Business Associate's obligations extend to acts and omissions of its agents or subcontractors and agent(s) to the same extent as Business Associate's own acts and omissions. Business Associate shall not assert lack of privity as a defense.

(f) No Limitation/Caps for Certain Claims. No limitation of liability

(contractual or otherwise) shall apply to Business Associate's obligations under this Agreement with respect to: (i) Breach of Unsecured PROTECTED HEALTH INFORMATION or Security Incident; (ii) violation of confidentiality obligations; (iii) infringement/misappropriation of Covered Entity's IP or data; or (iv) Business Associate's gross negligence, fraud, or willful misconduct.

(g) Savings Clause. The indemnity in this Agreement shall be enforced to the maximum extent permitted by applicable law. If any portion is held invalid, the remaining provisions shall continue in full force.

2. Set-off and Survival.

All obligations of the Parties under this Agreement, including indemnification, confidentiality, and protection of Protected Health Information, shall survive the expiration or termination of this Agreement. The indemnity obligations specifically survive termination and remain enforceable thereafter. Covered Entity may set off any undisputed indemnified amounts against fees or other sums otherwise due to Business Associate. Covered Entity also reserves the right, at its own option and expense, to participate in the defense of any claim, action, or proceeding through counsel of its choosing.

3. Mitigation and Cooperation.

(a) Business Associate's Duty to Mitigate. Business Associate shall promptly and at its sole cost mitigate damages resulting from violating this Agreement or the HIPAA Rules caused by the Business Associate or its agents or subcontractors. Mitigation includes technical remediation, operational containment, restoration of affected systems/data, and all actions necessary to reduce harm to individuals and Covered Entity.

(b) Timeliness and Standards. Mitigation shall begin without unreasonable delay and in accordance with Business Associate's written incident-response procedures and the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information). Business Associate shall cooperate fully with Covered Entity and provide all information Covered Entity reasonably requests to complete the four-factor assessment under 45 CFR §164.402(2).

(c) Evidence Preservation. Business Associate shall preserve all potentially relevant logs, images, and records relating to any Security Incident or potential Breach for not less than six (6) years, and shall not destroy such evidence without Covered Entity's written consent.

4. Rights in Proprietary and Confidential Information.

(a) Ownership. As between the parties, Covered Entity retains all rights,

titles, and interests in and to the proprietary information, confidential information, and PROTECTED HEALTH INFORMATION provided to Business Associate. No rights are granted to Business Associate, its agent(s) or subcontractor(s), other than those expressly stated in this Agreement.

(b) Use Restrictions and No Analytics/AI Training. Business Associate shall not use Covered Entity's proprietary information, confidential information, or PROTECTED HEALTH INFORMATION for its own analytics, model training, product development, or other purposes as expressly authorized in writing by Covered Entity or permitted by law.

(c) Return/Destruction. Upon Covered Entity's request or upon termination/expiration, Business Associate shall return or securely destroy all Covered Entity information, including PROTECTED HEALTH INFORMATION, and certify completion within thirty (30) days, except as retention is Required by Law or a court order (in which case Business Associate shall continue to protect such information in accordance with this Agreement).

(d) Injunctive Relief. Business Associate acknowledges that unauthorized use or disclosure of Covered Entity's proprietary information, confidential information, or Protected Health Information may cause irreparable harm for which monetary damages are inadequate. Covered Entity is therefore entitled to injunctive or equitable relief without posting bond in addition to all other remedies.

(e) Covered Entity's Limitation of Liability. Except for Covered Entity's gross negligence, willful misconduct, or breach of payment obligations, Covered Entity shall have no liability to Business Associate for consequential, incidental, special, punitive, or indirect damages, loss of profits, or loss of data, whether in contract, tort, or otherwise, even if advised of the possibility. Nothing in this clause limits Business Associate's obligations under this Agreement.

5. Cyber Liability Insurance.

Business Associate shall, at its sole cost, maintain Cyber and Privacy Liability Insurance with limits of not less than Five Million Dollars ($5,000,000) per claim and in the aggregate. Coverage shall, at a minimum, include:

- Privacy Liability – wrongful collection, use, retention, or disclosure of Protected Health Information or other personally identifiable information ("PII");

- Network Security Liability – unauthorized access, malware, denial-of-service, data corruption, or system interruption;
- Media and Content Liability – infringement, defamation, or digital-content risks;
- Regulatory Defense and Fines – defense costs and penalties to the extent insurable by law; and
- Incident Response and Breach Expenses – forensic investigation, notification, call-center, credit-monitoring, and data-restoration costs.

The policy shall:

- Name the City of Los Angeles ("City"), its departments, officers, and employees as additional insured where available at no additional cost;
- Be primary and non-contributory to any coverage carried by the City;
- Include no exclusion for unencrypted data or for acts of subcontractors;
- Remain in effect throughout the term of this Agreement and for not less than two (2) years following termination; and
- Require the insurer to provide at least 30 days' prior written notice to the City of cancellation, non-renewal, or material modification.

Upon request, Business Associate shall provide the City with a certificate of insurance and endorsements evidencing compliance and shall cooperate with the City's risk-management and legal teams in any claim investigation or recovery.

6. Survival. The rights and obligations of the Parties under this Agreement, including those relating to the protection, return, or destruction of Protected Health Information, and any other provisions which by their nature should survive, shall survive the termination or expiration of this Agreement. Specifically, Business Associate's obligations with respect to the protection, use, disclosure, and retention of Covered Entity's Protected Health Information shall survive termination of this Agreement for as long as Business Associate retains any of such Protected Health Information and, in any event, for no less than six (6) years, consistent with 45 C.F.R. § 164.530(j)(2).

7. Retention. This Agreement shall remain in effect for (i) the duration of Contract, if one exists between the Parties; or (ii) if no Contract exists, for the duration of the Services performed under this Agreement; and in either case, until all Protected Health Information created or received under this Agreement is returned to or destroyed at the direction of the Covered Entity, in accordance with 45 C.F.R. § 164.504(e)(2)(J).

8. Notices. Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representatives as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return

receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to the appropriate Party as follows:

If to Covered Entity (for Breach Notification):

Drew Steinberg, Public Safety Risk Manager (HIPAA Privacy Officer)
Los Angeles Fire Department
Risk Management Section
201 N. Figueroa St., 12th Floor
Los Angeles, CA 90012
(213) 202-9880

If to Covered Entity LAFD (For all other Matters)

Jaime E. Moore, Fire Chief
Los Angeles Fire Department
200 N. Main St., Room 1800
Los Angeles, California 90012
(213) 978-3800
(213) 978-3814 Fax

And:

Emilio Rodriguez, Fire Administrator
Los Angeles Fire Department
200 N. Main St., Room 1630
Los Angeles, California 90012
(213) 978-3731
(213) 978-3414 Fax

And:

If to Business Associate:

Jeff Endebak, General Counsel
Harris & Harris, Ltd.
111 West Jackson Blvd., Suite 650
Chicago, IL 60604
(312) 350-5128

H. MISCELLANEOUS

1. Amendment and Compliance.

The Parties shall amend this Agreement as necessary to comply with the HIPAA Rules, the HITECH Act, and any other applicable law or regulation. Any modification must be in writing and signed by duly authorized representatives of both Parties.

2. Duration and Survival.

This Agreement remains in effect for the duration of the underlying Contract or MOU and continues thereafter for so long as Business Associate retains any Protected Health Information on behalf of Covered Entity. All obligations relating to the use, protection, disclosure, retention, and destruction of Protected Health Information survive termination until such Protected Health Information is securely destroyed in accordance with 45 C.F.R. §§ 164.504(e)(2)(J) and 164.530(j)(2).

3. Entire Agreement and Modification.

This Agreement, together with the underlying Contract, constitutes the entire agreement between the Parties regarding Protected Health Information. It supersedes all prior discussions or representations, oral or written. Any amendment or waiver must be in writing and executed by both Parties.

4. Governing Law.

Except to the extent pre-empted by federal law including HIPAA Rules, this Agreement and the rights and obligations of the Parties hereunder shall be governed by and construed in accordance with the laws of the State of California, consistent with the governing-law clause of the underlying Contract.

5. Assignment of Rights and Delegation of Duties. This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions to the contrary, however, Covered Entity retains the right to assign or delegate any of its rights or obligations hereunder to any City department or office in a manner consistent with the HIPAA Rules. Assignments made in violation of this provision are null and void.

6. Nature of the Agreement and Relationship of the Parties.

Nothing in this Agreement shall be construed to create (i) a partnership, joint venture, fiduciary, or employment relationship other joint business

relationship between the Parties or any of their affiliates.

7. No Waiver.

Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

8. Equitable Relief.

Any disclosure of misappropriation of Protected Health Information by Business Associate in violation of this Agreement will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure or breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate, and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.

9. Severability.

The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

10. No Third Party Beneficiaries.

Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.

11. Headings.

The descriptive headings of the articles, sections, subsections of this Agreement are inserted for convenience only, do not constitute a part of this Agreement and shall not affect in any way the meaning or interpretation of this Agreement.

12. Inconsistencies.

Any inconsistency between this Agreement's provisions and the HIPAA Rules, including all amendments, as interpreted by HHS, a court, or another regulatory agency with authority over the Parties, shall be interpreted according to the interpretation of HHS, the court, or the regulatory agency. Any provisions of this Agreement that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be adhered to as stated in this Agreement.

13. Regulatory References. A citation in this Agreement to the Code of Federal Regulations shall mean the cited section as that section may be amended from time to time.

[SIGNATURE PAGE ON NEXT PAGE]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives.

THE CITY OF LOS ANGELES,
a Municipal Corporation

The signatory below has no personal, financial, beneficial, or familial interest in the contract.

By: Jaime E Moore
Jaime E. Moore
Los Angeles Fire Department
Fire Chief

Date: 4/13/26

APPROVED AS TO FORM:
HYDEE FELDSTEIN SOTO,
City Attorney

By:
Benjamin Benhan
Deputy City Attorney

Date: 4-16-2026

ATTEST:
PATRICE Y. LATTIMORE, City Clerk

By: Michael Vukelich
Deputy City Clerk

Date: Apr 16, 2026

HARRIS & HARRIS, LTD.,
An Illinois Corporation

By:
David M. Peters
Chief Executive Officer

Date: 4/8/26

By:
Doug Black
Chief Financial Officer

Date: 4/8/26

*Approved signature methods for California corporations:

1) Two signatures: One of the Chairman of the Board of Directors, President, or Vice President, and one of the Secretary, Chief Financial Officer, or Assistant Treasurer.

2) One signature of a Corporate-designated individual together with a properly attested resolution of the Board of Directors authorizing the individual to sign.

Agreement Number: C-204559

Annex A – Description of Services

(Attachment A to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and Harris & Harris, Ltd. ("Business Associate").

A.1. General Information

Field	Information to be completed by Business Associate
Business Associate Legal Name	**Harris & Harris, Ltd.**
Primary Contact (Name / Title)	**David M. Peters, President & CEO**
Email / Phone	**dpeters@harriscollect.com 630-777-7513**
Business Address / Principal Office	**111 W. Jackson, Suite 650, Chicago, IL 60604**
Effective Date of Services	**Ongoing**
City Department(s) Receiving Services	**Fire Department**
Related Contract / MOU Reference No.	**C-138561**

A.2. **Description of Services:** Provide a concise summary of the services Business Associate will perform on behalf of the City that involve access to, or the handling of, Protected Health Information (PHI).

City Department / Program	Description of Services Provided	Intended Purpose (e.g., Treatment, Payment, Operations)
Fire Department	Collection of unpaid transport fees and service charges, skip tracing patients and guarantors	Payment

(Note: Detailed data processing activities—including PHI elements, systems, and subcontractors—are documented in Annex B.)

A.3. **Key Deliverables:** List or describe deliverables to be produced under these services (e.g., billing reports, claims extracts, analytics summaries, audit logs, incident notifications).

Deliverable	Output Format	Frequency Recipient within City
Invoices, Remittance Report	Excel	Monthly
Performance Reports, Acknowledgement Report	Excel	Monthly
Returned Accounts Report	Excel	When Applicable

A.4. **Authorized Personnel:** Identify key individuals responsible for program delivery and compliance.

Role / Function	Name/Title/Email/Phone/Contact Info.
Client Service Oversight	**Kathy Dumont/Client Success Executive/ kdumont@harriscollect.com/916-698-1959**
Collection Services Oversight	**Carol Yakel/Director of Government Collections/ cyakel@harriscollect.com/585-409-1207**
Client Service	**Karla Ortega/Client Success Supervisor/ kortega@harriscollect.com/773-523-4099**

A.5. **Subcontractor Overview:** Provide a list of agents or subcontracts handling PHI on behalf of Business Associate.

Subcontractor / Agent Name	Service Provided	Contact Information	Physical / Hosting Location	Access to PHI (Y/N)	Copy of Sub-Business Associate Agreement on File (Y/N)	CE Approval Date

A.6. **Change Management:** Business Associate shall notify CE **in writing** of any change to the services, scope, or subcontractor relationships described in this Annex A **within ten (10) business days** of such change.

Annex B – Data Processing Activities

(Attachment B to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and Harris & Harris, Ltd. ("Business Associate").

B.1. **Overview:** This Annex documents the specific processing activities performed by the Business Associate on behalf of the City of Los Angeles ("Covered Entity") that involve the creation, receipt, maintenance, or transmission of PHI, as required by 45 C.F.R. § 164.504(e).

B.2. Categories of PHI Processed

☐ Demographic data ☐ Medical / clinical ☒ Claims / billing ☐ Employee occupational health ☐ Limited data set ☐ Other (specify): _____

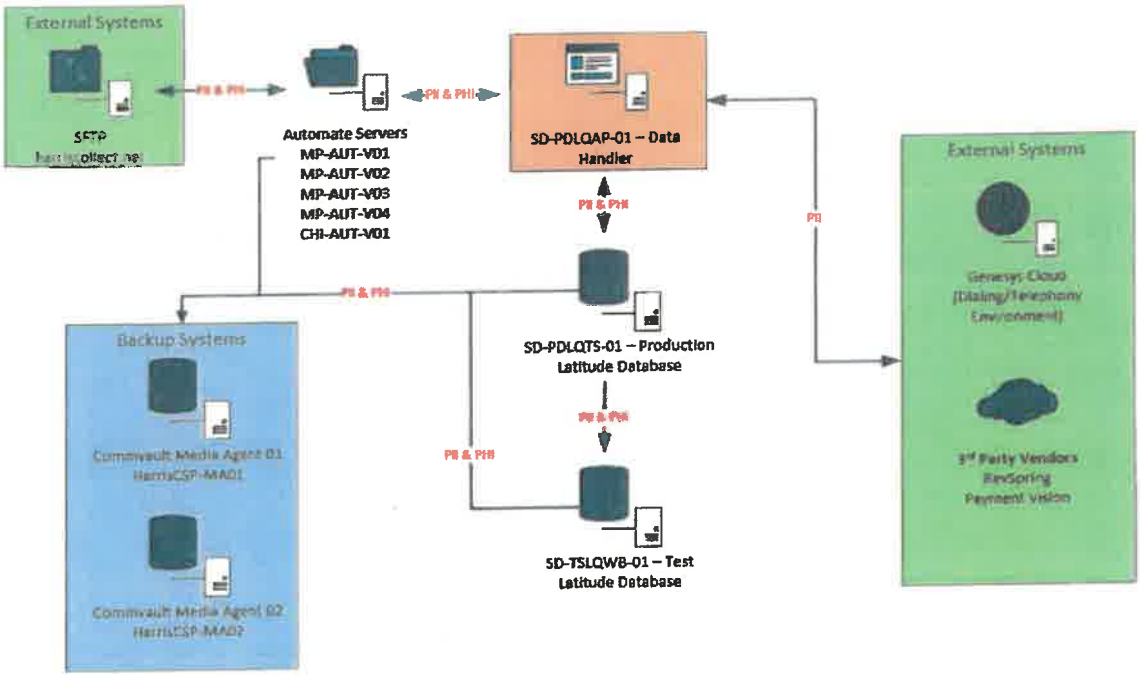
B.3. Data Processing Inventory

Activity/Function	Type of PHI Processed	Source of PHI (CE system or department)	Purpose of Processing	Retention Period
Collection Workflow	**Data elements such as Phone number, Account Number, SSN, DOB, DOD, Geographic Information, Insurance Number**	**LA EMS**	**Collections Services**	**7 Years**

B.4. Systems and Storage Environments

System / Application Name	Hosted By (Business Associate / Subcontractor / Cloud Provider)	Location (city/state or region)	Data Format (e.g., SQL, CSV)	Encryption at Rest (Y/N)	Encryption in Transit (Y/N)
Latitude	**Business Associate**	**Dallas TX**	**SQL**	**Y**	**Y**

B.5. **Data Flow Summary:** Provide a general narrative or attach a diagram showing how PHI flows through your environment—from collection or receipt to storage, processing, disclosure, and destruction.



B.6. **Safeguards Summary:** Summarize or reference your latest risk assessment.

- **Administrative Controls:** Policies, training, user access reviews
- **Physical Controls:** Facility security, media handling
- **Technical Controls:** Encryption, firewalls, MFA, logging

We maintain a robust security program designed to protect sensitive data across all areas of our organization. All data security and handling policies are reviewed and updated at minimum annually to ensure they reflect current standards and requirements.

Every new hire receives comprehensive data security training at the time of onboarding, covering the handling of PHI, PCI, PII, FTI, and CPNI. This training is refreshed annually for all staff and updated on an as-needed basis to address evolving requirements.

User access is managed in accordance with ISO, PCI DSS and NIST frameworks and standards, with formal access reviews conducted on a quarterly basis to ensure appropriate access controls are maintained at all times.

Our physical security posture is equally rigorous. All office locations are protected by

camera surveillance and badge access systems, with access granted strictly on a need-to-be-present basis. Network infrastructure closets are further secured with biometric access controls limited to authorized personnel only.

On the technical side, we deploy enterprise-grade firewalls and require multi-factor authentication (MFA) for all internal system logins. All encryption used to protect data at rest and in transit is FIPS 140-2 compliant, and system logs are retained for a full seven years to support audit and compliance requirements.

B.7. **Retention and Disposal**

Data Type	Retention Period	Disposal Method (e.g., shredding, cryptographic wipe)	Responsible Party
PII	**7 Years**	**NIST 800-88 Guidelines for a Purge in SQL**	**Business Associate**
PHI	**7 Years**	**NIST 800-88 Guidelines for a Purge in SQL**	**Business Associate**

B.8. **Change and Notification Obligations:** Business Associate must promptly notify Covered Entity of:

- Any addition / change of subcontractor or system involving PHI;
- Any change in storage location or data flow; or
- Any security incident as defined in 45 C.F.R. § 164.304.

B.9. **Certification:** Business Associate certifies that:

- The information in this Annex B is complete and accurate;
- All systems and subcontractors listed comply with the HIPAA Security Rule (45 C.F.R. §§ 164.308–164.312); and
- Business Associate will provide an updated Annex B within ten (10) business days of any material change.

Annex C – Security Incident and Breach Information

(Attachment C to the Business Associate Agreement (Agreement) between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity" or "CE") and Harris & Harris, Ltd. ("Business Associate").

C.1. **Purpose:** This Annex documents how Business Associate will detect, report, and coordinate with the City of Los Angeles ("Covered Entity") in the event of a Security Incident or Breach involving Protected Health Information (PHI) or electronic PHI (ePHI). It also serves as the template for incident notification and post-incident documentation.

C.2. Key Regulatory References

- 45 C.F.R. § 164.304 – Definition of "Security Incident."
- 45 C.F.R. § 164.308(a)(6) – Security Incident procedures (response & reporting).
- 45 C.F.R. § 164.402–410 – Breach Notification Rule requirements.

C.3. Designated Points of Contact

Role	Organization	Name / Title	Email / Phone	24/7 Contact (Y/N)
Business Associate Incident Response Lead	Business Associate	**Bob Mudd – Manager IT Infrastructure, Architecture and Security**	bmudd@harriscollect.com +1 312-460-3907	**N**
Business Associate Security Officer	Business Associate	**Bryan Albertson – CIO/CISO**	balbertson@harriscollect.com +1 312-423-7428	**Y**
Business Associate Privacy Officer	Business Associate	**Bryan Albertson – CIO/CISO**	balbertson@harriscollect.com +1 312-423-7428	**Y**
CE HIPAA Privacy Officer	City of Los Angeles			
CE CISO / ITA Cyber Ops	City of Los Angeles			

C.4. Reporting Obligations

Event Type	Initial Notice Due to CE	Content Required	Follow-Up Report Due
Suspected Security Incident	Within 72 hours of discovery	Description, date/time, systems/data involved, containment actions, contact person	Within 5 business days with preliminary findings

Confirmed Security Incident	Immediate (≤ 72 hours)	Expanded details, root cause in progress	Within 5 business days with root-cause analysis + corrective plan
Breach of Unsecured PHI (45 C.F.R. § 164.402)	Immediate notification (≤ 72 hours)	All data elements required under § 164.410(c): nature of PHI, individuals affected, timing, mitigation, actions taken	Comprehensive written report within 10 business days
Suspected Security Incident	Within 72 hours of discovery	Description, date/time, systems/data involved, containment actions, contact person	Within 5 business days with preliminary findings

C.5. **Incident Information Form:** *(to be completed by Business Associate and submitted with initial notice)*

Field	Information to be Provided by Business Associate
Date / Time Discovered	
Date / Time Occurred (if known)	
Detection Method (e.g., SIEM alert, user report)	
Type of Incident (e.g., ransomware, phishing, unauthorized access)	
Systems / Applications Affected	
Approx. Records Affected (# individuals)	
Containment Actions Taken	
Current Status (ongoing, contained, eradicated)	
External Parties Notified (LE, regulators, insurers)	
Evidence Preservation Steps	
Incident Lead Name / Contact	

(Attach additional pages or supporting documentation as needed.)

C.6. **Coordination and Investigation**

- Joint Response: Business Associate shall cooperate fully with CE, its designated representatives, and law enforcement in investigating and remediating any incident.
- Evidence Preservation: Business Associate must preserve logs, emails, forensic images, and related records for at least six (6) years from discovery of the incident.
- No Public Statements: Business Associate shall not make any public disclosure about the incident without CE's written consent.

C.7. **Breach Determination and Notification:** If Business Associate determines—or CE reasonably believes—that an incident constitutes a Breach of Unsecured PHI, Business Associate shall:

1. Immediately notify CE as above;

2. Provide CE with a draft notification package containing all information required by 45 C.F.R. § 164.410(c); and
3. Refrain from issuing any notifications to individuals or regulators without CE's written direction.

C.8. **Corrective Action and Lessons Learned:** Within ten (10) business days after incident closure, Business Associate shall submit to CE a written Root Cause Analysis and Corrective Action Plan, including any security control changes, training, or policy updates implemented as a result of the incident.

C.9. **Ongoing Reporting and Metrics:** Business Associate shall provide to CE, upon request:

- A summary of all Security Incidents for the preceding twelve (12) months (including near misses);
- Evidence of incident response testing or tabletop exercises performed within the past year; and
- Contact updates for incident response personnel.

C.10. **Certification:** The Business Associate certifies that:

- It has established, documented, and tested incident response procedures consistent with 45 C.F.R. § 164.308(a)(6);
- All information reported herein is accurate to the best of its knowledge; and
- It will promptly update this Annex should its incident response contacts or procedures change.

Annex D – Artificial Intelligence ("AI") System and Automated Processing

(Attachment B to the Business Associate Agreement ("Agreement") between the City of Los Angeles by and through Los Angeles Fire Department ("Covered Entity") and Harris & Harris, Ltd. ("Business Associate").

D.1. **Purpose:** This Annex documents and governs AI System, Machine Learning ("ML"), or other automated data-processing activities performed by Business Associate that exclusively involve, rely upon, or are derived from Protected Health Information entrusted by the City of Los Angeles. (To the extent AI System and Automated Processing does not involving Protected Health Information, Business Associate's general AI system activities fall outside the scope of this Agreement.)

D.2. **Key Regulatory References**

- 45 C.F.R. §§164.308-312 (security safeguards).
- 45 C.F.R. §164.514(b) (de-identification methodology), and
- Applicable state or municipal data-governance laws (e.g., California Privacy Rights Act, California AI procurement guidance).

D.3. **Definitions**

Applicable definitions describing AI System, Automated Processing, or Automated Decision Systems (ADS) are outlined in the Definition Section of the Agreement.

D.4. Disclosure of AI or Automated Processing *(to be completed by Business Associate)*

System/Tool name	Vendor/Deployer	Purpose/Use Case	PHI Input or Derived Data Used Categories	Output/Decisions Produced	Human Intervention
N/A					

D.4. **Authorized and Prohibited Uses**

Authorized uses with Covered Entity's written approval:

- Performing Covered Entity-approved treatment, payment, or health-care operations under 45 C.F.R. §164.506(c).
- Performing limited quality or operational analytics solely for Covered Entity's benefit.

Prohibited uses:

- Training, fine-tuning, or validating general-purpose, commercial, or generative AI models.
- Combining Covered Entity with other clients' data or external sources.
- Creating synthetic or de-identified data for independent use without Covered Entity's written authorization.

- Any automated decision that affects individuals without human review or Covered Entity's oversight.

D.5. **Transparency and Documentation**

- Provide plain language description of each AI/ADS system's purpose, inputs and logic request:

- Provide documentation of de-identification methodology (Expert Determination or Safe Harbor) per 45 C.F.R. §164.514(b).

- Provide proof that you maintain internal model-risk and bias-assessment documentation, updated annually or after any material change where Covered Entity's data, including PHI, is in scope.

D.6. **Safeguard and Data Integrity**

Business Associate shall:

- Apply HIPAA Security Rule safeguards (45 C.F.R. §164.308-312) to all systems using or storing PHI.
- Encrypt PHI at rest and in transit (FIPS 140-2 or successor).
- Implement logging, access control, and audit trails for training, inference, and model-output use.
- Ensure segregation of Covered Entity PHI datasets from test or sandbox, other clients, or public data environments.
- Monitor for model drifts, data leakages, inversions, or biases and report material findings to Covered Entity.

D.7. **Subcontractors and AI Vendors**: List any third parties or vendors supporting AI or automated processing of PHI.

Subcontractor/Vendor Name	Role/Function	System or Model Used	Location/Hosting Region
N/A			

All such parties must be bound by written agreements imposing HIPAA-equivalent obligations and are subject to CE's prior written approval.

D.8. **Incident Reporting**: Any algorithmic malfunction, bias event, unauthorized access (to the data, model, test/production env., etc.), or other incident affecting PHI integrity or system behavior shall be treated as a Security Incident under Annex C and reported within the same timelines.

D.9. **Oversight and Audit**

Covered Entity may:

- Audit Business Associate's AI systems and related controls.
- Require suspension of any high-risk automated processing.
- Request copies of model documentation and validation results.

D.10. **Certification**

The Business Associate certifies that:

- All AI and automated systems handling Covered Entity data comply with HIPAA, this Agreement, and applicable laws, standards and policies.
- Covered Entity will be notified within ten (10) business days of any new or materially changed automated-processing activity.
- Human oversight (including Human-in-the-loop and Human-on-the-loop) and decision transparency, fairness, and accountability are maintained at all times.