

SECOND AMENDATORY AGREEMENT

THIS SECOND AMENDATORY AGREEMENT is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (“City”) and **ROLAND PROCESS SERVICE & INVESTIGATIONS, LLC**, a Colorado limited liability company, with its principal business located at 1600 Albion Street, Suite 204, Colorado Expo Building, Denver, Colorado 80222 (“Contractor”), collectively “the Parties.”

RECITALS:

A. The Parties entered into an agreement dated December 10, 2015, and amended the agreement on April 28, 2017 (“Agreement”) to provide service of legal process services.

B. The Parties desire to amend the Agreement to incorporate additional requirements into the Scope of Work.

NOW THEREFORE, in consideration of the premises and the Parties’ mutual covenants and obligations, the Parties agree as follows:

1. The Privacy and Data Security Safeguards shall incorporate additional requirements into the Scope of Work of the Agreement. The Privacy and Data Safeguards marked as **Exhibit C** is attached hereto and incorporated by this reference.

2. As herein amended, the Agreement is affirmed and ratified in each and every particular.

3. This Second Amendatory Agreement will not be effective or binding on the City until it has been fully executed by all required signatories of the City and County of Denver, and if required by Charter, approved by the City Council.

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Contract Control Number: ATTNY-201525605-02

Contractor Name: ROLAND PROCESS SERVICE &
INVESTIGATIONS, LLC

By: James D Roland

Name: *James D Roland*
(please print)

Title: Operations Manager
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)



Contract Control Number:

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of

SEAL

CITY AND COUNTY OF DENVER

ATTEST:

By _____

APPROVED AS TO FORM:

REGISTERED AND COUNTERSIGNED:

By _____

By _____

By _____



Exhibit C
Privacy and Data Security Safeguards
(Covered Entity-Business Associate)

City is hereinafter referred to as “Covered Entity”. Roland Process Service & Investigations, LLC. dba Denver Attorney Services, LLC is hereinafter referred to as “Business Associate”. The purpose of these terms is to assure privacy and data security safeguards.

Part I
Protected Health Information – HIPAA/HITECH/Privacy Rule

A. Covered Entity and Business Associate have entered into an arrangement (the “Business Arrangement”), pursuant to which Business Associate may provide services that require it to view, access, deliver, and use health and other information that is protected by state and/or federal law.

B. Pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the U.S. Department of Health & Human Services (“HHS”) promulgated the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Standards”), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards (each a “Covered Entity,” or collectively, “Covered Entities”) to protect the privacy of certain individually identifiable health information (“Protected Health Information,” or “PHI”).

C. Pursuant to HIPAA, HHS has issued the Security Standards (the “Security Standards”), at 45 C.F.R. Parts 160, 162 and 164, for the protection of electronic protected health information (“E PHI”).

D. The City is a Covered Entity and to protect the privacy and security of PHI, including E PHI, created or maintained by or on behalf of City and their clients and others, the Privacy Standards and Security Standards require a Covered Entity to enter into a “Business Associate agreement” with certain individuals and entities providing services for or on behalf of Covered Entity if such services require the use or disclosure of PHI or E PHI.

E. February 17, 2009, the federal Health Information Technology for Economic and Clinical Health Act was signed into law (the “HITECH” Act”), and the HITECH Act imposes certain privacy and security obligations on Covered Entities in addition to the obligations created by the Privacy Standards and Security Standards.

F. The HITECH Act revises many of the requirements of the Privacy Standards and Security Standards concerning the confidentiality of PHI and E PHI, including extending certain HIPAA and HITECH Act requirements directly to Business Associates.

G. The HITECH Act requires that certain of its provisions be included in Business Associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon Business Associates as well as Covered Entities.

H. The Parties desire that Business Associate obtain access to such PHI and/or EPHI in accordance with the terms specified herein, whether such access occurs from Covered Entities or Business Associate.

I. The Parties also recognize and agree to comply with other laws and industry standards for the protection of other confidential information.

J. The Parties incorporate the following terms as part of their Agreement.

1. Obligations of Business Associate.

1.1 Business Associate may receive from Covered Entity, or create or receive on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including, without limitation, PHI and EPHI. All capitalized terms not otherwise defined in this Agreement shall have the meanings set forth in the Privacy Standards, Security Standards or the HITECH Act, as applicable (collectively referred to hereinafter as the “Confidentiality Requirements”). All references to PHI herein shall be construed to include EPHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Confidentiality Requirements if the PHI were used or disclosed by Covered Entity in the same manner. Business Associate shall use appropriate safeguards to prevent the use or disclosure of PHI other than as expressly permitted under this Agreement.

1.2 Business Associate will implement administrative physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate acknowledges that the HITECH Act requires Business Associate of Covered Entity to comply with 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as if Business Associate were the Covered Entity, and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act. Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to ensure that the technology safeguards used by Business Associate to secure PHI will render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology (“NIST”) concerning the protection of identifiable data such as PHI. Lastly, Business Associate will promptly report to Covered Entity any Security Incident of which it becomes aware. At the request of City, Business Associate shall identify: the date of the Security Incident, the scope of the Security Incident, the Business Associate’s response to the Security Incident and the identification of the party responsible for causing the Security Incident, if known.

2. Use of PHI. Except as otherwise required by law, Business Associates of Covered Entity shall use PHI (i) solely for Covered Entity's benefit and only for performing services for Covered Entity as such services are defined in Business Arrangements, and (ii) as necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, provided that such uses are permitted under federal and state law. Covered Entities shall retain all rights in the PHI not granted herein. Except to the extent necessary to perform its obligations under the Business Arrangements, Business Associates may not de-identify PHI received from, or created on behalf of Covered Entity without the express written authorization of Covered Entity. Covered Entity hereby consents to de-identification of PHI by Business Associate solely for use by Business Associate or its affiliate of such de-identified PHI in medical research, peer review and quality assurance activities, without regard to whether such activities are conducted for or in conjunction or affiliation with Covered Entity.

3. Disclosure of PHI. Subject to any limitations in this Agreement, Business Associate may disclose PHI to any third-party persons or entities as necessary to perform its obligations under the Business Arrangement and as permitted or required by applicable federal or state law. Further, Business Associate may disclose PHI for the proper management and administration of the Business Associate provided that (i) such disclosures are required by law, or (ii) Business Associate: (a) obtains reasonable assurances from any third party to whom the information is disclosed that it will be held confidential and further used and disclosed only as required by law or for the purpose for which it was disclosed to the third party; (b) agrees to immediately notify Covered Entity of any instances of which it is aware that PHI is being used or disclosed for a purpose that is not otherwise provided for this Agreement or for a purpose not expressly permitted by the Confidentiality Requirements. Additionally, Business Associate shall ensure that all disclosures of PHI by Business Associate and the third party comply with the principle of "minimum necessary use and disclosure," i.e., only the minimum PHI that is necessary to accomplish the intended purpose may be disclosed. Business Associate shall comply with Section 13405(b) of the HITECH Act, and any regulations or guidance issued by HHS concerning such provision, regarding the minimum necessary standard and the use and disclosure (if applicable) of Limited Data Sets. If Business Associate discloses PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to agents, including a Business Associate for the Business Associate (collectively "Recipients"), Business Associate shall require Recipients to agree in writing to the same restrictions and conditions that apply to the Business Associate under this Agreement. Business Associate shall report to Covered Entity any use or disclosure of PHI not permitted by this Agreement, of which it becomes aware. Such report shall be made within three (3) business days of the Business Associate becoming aware of such use or disclosure. In addition to Business Associate's obligations under Section 9, Business Associate agrees to mitigate, to the extent possible (and unless otherwise required by Covered Entity) in writing any harmful effect that is known to Business Associate and is the result of a use or disclosure Business Associate or Recipients in violation of this Agreement. Business Associate's report will be provided to the Covered Entity on the same day, and the Covered Entity will be the final authority on if the breach was mitigated appropriately.

4. Individual Rights Regarding Designated Record Sets. If Business Associate maintains a Designated Record Set on behalf of Covered Entity, Business Associate shall (i) provide access to, and permit inspection and copying of, PHI by Covered Entity or, if so directed by Covered Entity, an individual who is the subject of the PHI under conditions and limitations required under 45 C.F.R. § 164.524, as it may be amended from time to time, and (ii) amend PHI maintained by Business Associate as requested by Covered Entity. Business Associate shall respond to any request from Covered Entity for access by an individual within five (5) days of such request and shall make any amendment requested by Covered Entity within ten (10) days of such request. Any information requested under this Section 4 shall be provided in the form or format requested, if it is readily producible in such form or format. Business Associate may charge a reasonable fee based upon the Business Associates labor costs in responding to a request for electronic information (or a cost-based fee to produce non-electronic media copies). Covered Entity shall determine whether a denial is appropriate or an exception applies. Business Associate shall notify Covered Entity within five (5) days of receipt or any requests for access or amendment by an individual. Covered Entity shall determine whether to grant or deny any access or amendment requested by the individual. Business Associate shall have a process in place for receiving requests for amendments and for appending such requests to the Designated Record Set, as requested by Covered Entity.

5. Accounting for Disclosures. Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI with respect to the individual, in accordance with 45 C.F.R. § 164.528, as amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision. Business Associate shall provide to Covered Entity such information necessary to provide an accounting within thirty (30) days of Covered Entity's request or such shorter time as may be required by state or federal law. Such accounting must be provided without cost to the individual or to Covered Entity if it is the first accounting requested by an individual within any twelve (12) month period; however, a reasonable fee based on Business Associate's labor costs in responding to a request for electronic information (or a cost-based fee for the production of non-electronic media copies) may be charged for subsequent accountings within the same twelve (12) month period so long as Business Associate informs Covered Entity and Covered Entity informs Covered Entities and individual in advance of the fee, and the individual is afforded an opportunity to withdraw or modify the request. Such accounting obligations shall survive termination of this Agreement and shall continue if Business Associate maintains PHI. Business Associate shall notify Covered Entity within five (5) days of receipt of any request from an individual for an accounting of disclosures.

6. Withdrawal of Authorization. If the use or disclosure of PHI in this Agreement is based upon an individual's specific authorization for the use of his or her PHI, and (i) the individual revokes such authorization in writing, (ii) the effective date of such authorization has expired, or (iii) the consent or authorization is found to be defective in any manner that renders it invalid, Business Associate agrees, if it has received notice of such revocation or invalidity, to cease the use and disclosure of any such individual's PHI except to the extent it has relied on such use or disclosure, or where an exception under the Confidentiality Requirements expressly applies.

7. **Records and Audit.** Business Associate shall make available to Covered Entity or its Covered Entity clients or its agents, its internal practices, books, and records relating to the use and disclosure of PHI accessed, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity's compliance with the Confidentiality Requirements, such internal practices, books and records to be provided in the time and manner designated by Covered Entity and its Covered Entity clients and its agents. Except to the extent prohibited by law, Business Associate agrees to notify Covered Entity immediately upon receipt by Business Associate of any and all requests by or on behalf of any and all federal, state, and local government authorities served upon Business Associate for PHI subject to this Agreement.

8. **Confidentiality.** Business Associate shall take any steps reasonably required, including, but not limited to, those actions enumerated herein, to (i) protect PHI from unauthorized uses or disclosures, and (ii) maintain the confidentiality and integrity of PHI.

9. **Data Breach Notification and Mitigation.**

9.1 HIPAA Data Breach Notification and Mitigation. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. § 164.402 (hereinafter a "HIPAA Breach"). The Parties acknowledge and agree that 45 C.F.R. § 164.404, as described below in this section 9, governs the determination of the date of a HIPAA Breach. In the event of any conflict between this Section 9 and the Confidentiality Requirements, the more stringent requirements shall govern. Business Associate will, following the discovery of a HIPAA Breach, notify Covered Entity immediately and in no event later than three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. § 164.412 concerning law enforcement investigations. For purposes of reporting a HIPAA Breach to Covered Entity, the discovery of a HIPAA Breach shall occur as of the first day on which such HIPAA Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a HIPAA Breach if the HIPAA Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the HIPAA Breach) who is an employee, officer or other agent of the Business Associate. No later than seven (7) business days following a HIPAA Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity, as appropriate, to comply with the HIPAA Breach notification requirements set forth at 45 C.F.R. § 164.400 et seq. Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered

Entity with: (i) contact information for individuals who were or who may have been impacted by the HIPAA Breach (e.g., first and last name, mailing address, street address, phone number, email address); (ii) a brief description of the circumstances of the HIPAA Breach including the date of the HIPAA Breach and the date of discovery; (iii) a description of the types of unsecured PHI involved in the HIPAA Breach (e.g. names, social security number, date of birth,, address(es), account numbers of any type, disability codes, diagnostic and/or billing codes and similar information); (iv) a brief description of what the Covered Entity has done or is doing to investigate the HIPAA Breach, mitigate harm to the individual impacted by the HIPAA Breach, and protect against future HIPAA Breaches; and (v) appoint a liaison and provide contact information for same so that Covered Entity may ask questions or learn additional information concerning the HIPAA Breach. Following a HIPAA Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the HIPAA Breach, including but not limited to the information described in items (i) through (v), above.

9.2 Data Breach Notification and Mitigation Under Other Laws. In addition to the requirements of Section 9.1, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach of individually identifiable information (including but not limited to PHI, and referred to hereinafter as “Individually Identifiable Information”) that, if misused, disclosed, lost or stolen, Covered Entity believes would trigger an obligation under one or more State data breach notification laws, (each a “State Breach”) to notify the individuals who are the subject of the information. Business Associate agrees that in the event of any Individually Identifiable Information is lost, stolen, used or disclosed in violation of one or more State data breach notification laws, Business Associate shall promptly: (i) cooperate and assist Covered Entity and/or their Covered Entity clients with any investigation into any State Breach or alleged State Breach; (ii) cooperate and assist Covered Entity and/or their Covered Entity clients with any investigation(s) into any State Breach or alleged State Breach conducted by any State Attorney General or State Consumer Affairs Department (or their respective agents); (iii) comply with Covered Entity’s and/or their Covered Entity client’s determinations regarding the Parties’ obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the State Breach; and (iv) assist with the implementation of any decision by Covered Entities or any State agency, including any State Attorney General or State Consumer Affairs Department (or their respective agents), to notify individuals impacted or potentially impacted by a State Breach.

10. Duties on Termination. Upon termination of this Agreement for any reason, Business Associate agrees either to: return all PHI to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents. Business Associate shall timely provide Covered Entity a certification of what PHI was destroyed. If the data is paper and shredded, it must be shredded to NIST standards as set forth in Table A of this link: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf> (Table A-1) by destroying the paper using cross cut shredders which produce particles that are 1 mm x 5 mm in. x 0.2 in. in size (or smaller), or pulverizing/disintegrating paper materials using a disintegrator device equipped with a 3/32 in. (2.4 mm) security screen. In the case of PHI which is not feasible to “return or destroy,” Business Associate shall extend the protections of this Agreement to such PHI and shall limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long Business Associate maintains such PHI; provided that Business Associate may continue to hold and use de-identified PHI as set forth above. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatments of such PHI.

11. Transporting or Storing Documents. Documents shall be transported or stored securely, including using locked premises/bin(s) or bag(s).

12. Hiring and Training. Business Associate shall engage persons who already have sufficient training and experience to comply with the Covered Entity’s contract requirements, including NIST and/or CFR standards. Business Associate may also provide training to qualify and maintain qualification of its employees, contractors, and subcontractors to provide services under this Agreement.

13. Other Types of Confidential Information. The Parties agree that in addition to the protection of PHI, Business Associate shall use the above or equivalent practices and procedures for the safeguarding of other confidential personally identifiable information (“PII”), and shall adhere to any other particularized privacy and data protection laws pertinent to the work under this Agreement.

14. Equitable Relief. Business Associate understands and acknowledges that any disclosure or misappropriation of any PHI or other PII in violation of this Agreement would cause irreparable harm, the amount of which may be difficult to ascertain, and 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 any such further disclosure or breach and for such other relief as Covered Entity shall deem appropriate. Such right of Covered Entity is in addition to the remedies otherwise available 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.