

**Amendment No.: 3**

**TO CONTRACT NO.: DMS 10/11-011  
BETWEEN  
UNITED HEALTHCARE OF FLORIDA, INC.  
AND THE FLORIDA DEPARTMENT OF MANAGEMENT SERVICES**

This Amendment to Contract No.: DMS 10/11-011 (the "Contract") is by and between United Healthcare of Florida, Inc. (the "Service Provider") and the State of Florida acting through the Department of Management Services (the "Department") (collectively the "Parties").

**WHEREAS**, the Department awarded the Contract to Service Provider for the provision of group health maintenance organization (HMO) services pursuant to the Invitation to Negotiate requirements in Section 110.123(3)(h)8.a, Florida Statutes.

**WHEREFORE**, the Parties do hereby agree to amend the Contract by October 10, 2014, as follows:

1. Attachment A: Performance Guarantees. The Department does hereby amend the Contract to replace Performance Guarantee numbers 5, 15, 16, 17 and 18 associated with the Contract with the Performance Guarantees in Attachment A, effective January 1, 2015.
2. Attachment B: Warranty of Security. The Department does hereby amend the Contract to replace Section 3.3.5, Employee and Subcontractor Security Requirements, with Attachment B. In the event the Contract and the Warranty of Security provision conflict, the Warranty of Security shall control. Attachment B is effective January 1, 2015.
3. Attachment C: Combined HIPAA Privacy Business Associate Agreement and Confidentiality Agreement and HIPAA Security Rule and Hitech Act Compliance Agreement. Attachment C is effective the earlier of the date of execution or September 24, 2014.
4. Attachment D: Affidavit of Best Pricing. Attachment E is effective January 1, 2015.
5. Attachment E: Affidavit of No Off-shoring of Data. Attachment D is effective upon execution.
6. Attachment F: Section 3.3.6 Work Locations; No Off-shoring of Data. The Department does hereby amend Section 3.3.6 of the Contract to add after the current last paragraph the provisions set forth in Attachment F. Attachment F is effective upon execution.
7. Attachment G: Administrative Requirement (AR) #20, Member Handbook or Certificate of Coverage. The Department does hereby amend AR #20 with the following passage. This paragraph and Attachment G, Summary Plan Description Template, are effective upon execution for plan documents pertinent to Plan Year 2015.

Service Provider shall use an exact template of the state-approved Summary Plan Description (also called Member Handbook/Certificate of Coverage) for *State of Florida Employees' Group Insurance Program HMO Plan* with certain

document edits permitted for Service Provider's contact information and other limited information, as approved by the state, (i.e., processes unique to the Service Provider).

8. Anti-Kickback Statute. The Department does hereby amend the Contract to replace Section 11.5(b), Anti-Kickback Statute, with the following passage. This paragraph is effective upon execution.

Each party certifies that it will not violate the following laws with respect to the performance of its obligations under this Contract: the federal anti-kickback statute, set forth at 42 U.S.C§ 1320a-7b(b); Florida's Anti-Kickback Law, set forth at §409.920, Florida Statutes; the federal Stark law, set forth at 42 U.S.C. § 1395nn; the Patient Self-Referral Act of 1992, set forth at §456.053, Florida Statutes; the Patient Brokering Act, set forth at §817.505, Florida Statutes; and the Florida False Claims Act, set forth at §§ 68.081 – 68.092, Florida Statutes.

9. Amendment Number Correction. A scrivener's error was made previously wherein the Contract Renewal executed on July 24, 2013 was not numbered. The aforementioned Renewal should be Amendment #2.
10. Except as specifically enumerated herein, all other terms and conditions of the Contract shall remain in full force and effect.

IN WITNESS WHEREOF, the Parties hereto have caused this Amendment to be executed on the last date shown below.

DEPARTMENT OF MANAGEMENT SERVICES

(Signature)

C. Darren Brooks

Deputy Secretary, Workforce Management

Date:

10/15/14

UNITED HEALTHCARE OF FLORIDA, INC.

(Signature)

Print Name:

Dan Roche

Title: Regional Contract Manager

Date:

10/7/2014

**Attachment A: Performance Guarantees**

Effective January 1, 2015

PG #	Performance Indicator	Standard/Goal	Measurement Criteria	Frequency of Measurement	Liquidated Damages	Measurement Methodology (Formula used to measure results)
<b>I. Account Management</b>						
5.	Plan Performance Review	Within ten (10) calendar days following delivery of a performance review from the Department, the Vendor shall develop and submit a corrective action plan (CAP) approved by the Department, and implement such plan the time prescribed by the approved CAP.	Vendor shall submit an approvable CAP within ten (10) Calendar Days and implement as agreed upon in the CAP.	No specified frequency	\$2,500 per Calendar Day beyond ten (10) Calendar Days.	Measurement from the date of delivery of the Plan Performance Review in Calendar Days.

## Attachment A: Performance Guarantees

Effective January 1, 2015

PG #	Performance Indicator	Standard/Goals	Measurement Criteria	Frequency if Measurement	Liquidated Damages	Measurement methodologies (Formula used to measure results)
<b>VI. Claims Processing</b>						
15.	Claims Timeliness	Measured from the date the claim is received in the office (day 1) to the date the processed claim reaches final action determination (includes weekends and holidays).	<p>Average quarterly turn-around time for claims processing will not exceed:</p> <ul style="list-style-type: none"> <li>- Fourteen (14) calendar days for 90% of clean claims (non-investigated);</li> <li>- Thirty (30) calendar days for 99.5% of all claims.</li> </ul>	<p>Quarterly internal audit performed on all claims.</p> <p>Measured, reported, and reconciled quarterly.</p>	<p><u>a.) Clean claims:</u> \$1,000 for each full percentage point below the 90% required minimum standard within 14 days.</p> <p><u>b.) All claims:</u> \$1,000 for each full percentage point below the 99.5% required minimum standard within thirty (30) days.</p>	<p><u>a.) Clean claims:</u> 100% x (Total number of original claims processed within 14 days / total number of original claims processed during the quarter)</p> <p><u>b.) All claims:</u> 100% x (Total number of original claims processed within thirty (30) days / total number of original claims processed during the quarter)</p> <p>For electronically submitted claims, Day 1 is the date the claim was received, irrespective of the time of day and including weekends and holidays. For paper claims, Day 1 is the date that the claim was stamped upon receipt irrespective of the time of day and including weekends and holidays.</p>

**Attachment A: Performance Guarantees**

Effective January 1, 2015

PG #	Performance Indicator	Standard/Goals	Measurement Criteria	Frequency if Measurement	Liquidated Damages	Measurement methodologies (Formula used to measure results)
<b>VI. Claims Processing (continued)</b>						
16.	Financial accuracy	Measured as the absolute value of financial errors divided by the total paid value of audited dollars paid based on the quarterly internal audit of a statistically valid sample.	Average quarterly financial accuracy of 99% or greater.	Quarterly internal audit performed on all claims.  Measured, reported, and reconciled quarterly.	\$5,000 for each full percentage point below 99%.	(Amount of claims dollars in sample paid correctly / amount of claims dollars paid in sample) x (strata population dollars / total population dollars)
17.	Processing accuracy (claims)	Measured as the percent of claims processed without non-financial error.	Average quarterly processing accuracy of 95% or greater.	Quarterly internal audit performed on all claims.  Measured, reported, and reconciled quarterly.	\$5,000 for each full percentage point below 95%.	(Number of claims in strata sample without an administrative error / number of claims in sample) x (number of claims in strata population / number of claims in total population)
18.	Payment accuracy (claims)	Measured as the percent of claims processed without financial payment error.	Average quarterly payment accuracy of 97% or greater.	Quarterly internal audit performed on all claims.  Measured, reported, and reconciled quarterly.	\$5,000 for each full percentage point below 97%.	(number of claims in sample paid accurately / number of claims in sample) x (number of claims in strata population / number of claims in total population)

## **Attachment B: Warranty of Security**

### **Warranty of Security**

#### **A. Background Screening**

The Vendor shall ensure that a background screening is conducted on all Persons.

Definitions of capitalized terms as used herein:

“Access” means the ability and/or means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network containing State of Florida Data.

“State of Florida Data” means any representation of information, knowledge, facts, concepts, computer software, computer programs or instructions, whether said information is confidential information or personal health information. Data may be in any form, including but not limited to, in storage media, stored in the memory of the computer, in transit or presented on a display device, or a hard copy.

“Person” or “Persons” means employees, Subcontractor personnel, independent contractors, leased employees, volunteers, licensees or other individuals directly performing Services under the Contract whether or not the Person has access to State of Florida Data. The term Person or Persons also means those Persons who are not performing Services under the Contract but have access, including indirect access, to State of Florida Data. The term Subcontractor as used herein does not include persons who are licensed in the State where Services are being rendered to practice either dentistry or medicine.

The minimum background check process shall include a check of the following databases through a law enforcement agency or a professional background screener accredited by the National Association of Professional Background Screeners:

- Social Security Number trace; and
- Criminal Records (Federal, State and County criminal felony and misdemeanor, national criminal database for all States which make such data available);

The Vendor agrees that each Person will be screened prior to performing Services related the Contract or having Access to State of Florida Data. The Vendor is responsible for any and all costs and expenses in obtaining and maintaining the criminal background screening information for each Person described above. The Vendor and its Subcontractors shall maintain documentation of the screening and other requirements provided herein in the Person’s employment file. Within five (5) business days of receipt of a written request from the Department, the Vendor shall provide copies of all documentation of the security screening of any Person, including Subcontractor personnel. The Vendor and its Subcontractors shall abide by all applicable laws, rules and regulations including, but not limited to the Fair Credit Reporting Act and/or any equal opportunity laws, rules, regulations or ordinances.

The initial screenings shall be completed on all Persons no later than the Effective Date.

### **1. Disqualifying Offenses**

If at any time it is determined that a Person has a criminal misdemeanor or felony record including adjudication of guilt (a plea of guilty or nolo contendere, or a guilty verdict) within the last ten (10) years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Vendor is required to immediately remove that Person from any position with access to State of Florida Data or directly performing Services under the Contract. The disqualifying offenses are:

- Computer-related or information technology crimes
- Fraudulent practices, false pretenses and frauds
- Forgery and counterfeiting
- Violations involving checks and drafts
- Misuse of medical or personnel records

### **2. Self-Disclosure**

The Vendor shall require all Persons to self-report within three (3) business days of adjudication to the Vendor any adjudication of guilt as described in 1. above for the Disqualifying Offenses. The Vendor shall immediately disallow that Person Access to any State of Florida Data or from directly performing Services under the Contract. Additionally, the Vendor shall require that the Person complete an annual certification that he or she has not received an adjudication of guilt as described in 1. above for the Disqualifying Offenses and shall maintain that certification in the employment file.

### **3. Refresh Screening**

Every five years from the time initially performed for each Person during the Term of the Contract, a background screening as described in A. above shall be conducted.

### **4. Quarterly Reporting**

The Vendor is required to submit a written attestation to the Department within forty-five (45) days from the end of each quarter certifying compliance with this Amendment.

### **B. Duty to Provide Secure Data**

The Vendor shall maintain the security of State of Florida Data including, but not limited to, a secure area around any display of such data or data that is otherwise visible. The Vendor shall also comply with all HIPAA requirements and any other State and federal rules and regulations regarding security of information.

### **C. Department's Ability to Audit Screening Compliance and Inspect Locations**

The Department reserves the right to audit the Vendor's background screening process upon five (5) business days prior written notice to the Vendor during the Term of the Contract. The Department shall also have the right to inspect the Vendor's working area and/or location upon five (5) business days prior written notice to

the Vendor to ensure that access to the State of Florida Data is secure and in compliance with the Contract and all applicable State and federal rules and regulations.

Upon notice of a security breach as defined in the Business Associate Agreement, the Department shall have the right to audit the Vendor's background screening process upon twenty-four (24) hours written notice to the Vendor. This provision shall control over any conflicting provisions within the main Contract or the Business Associate Agreement.

#### **D. Indemnification**

The Vendor agrees to defend, indemnify and hold harmless the Department, the State of Florida, its officers, directors and employees for any claims, suits or proceedings alleging a breach of this Warranty of Security. Following a breach, as defined in the Business Associate Agreement between the Parties, the Vendor shall provide credit monitoring services at its own cost for a one (1) year period for those individuals affected or potentially affected by a breach of this Warranty of Security.



## Attachment C

### **COMBINED HIPAA PRIVACY BUSINESS ASSOCIATE AGREEMENT AND CONFIDENTIALITY AGREEMENT AND HIPAA SECURITY RULE ADDENDUM AND HITECH ACT COMPLIANCE AGREEMENT**

The Parties have entered into this Agreement for the purpose of satisfying the Business Associate contract requirements of the regulations at 45 Code of Federal Regulations (CFR) 164.502(e) and 164.504(e), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Security Rule, codified at 45 CFR Part 164, Subparts A and C, the Health Information Technology for Economic and Clinical Health Act (the HITECH Act, as enacted in Pub. L. No. 111-05 H.R., 111<sup>th</sup> Congress (2009), Title XIII), as well as the confidentiality requirements contained in section 110.123(9), Florida Statutes.

Term: This Agreement shall be effective as of the earlier of the date of execution or September 24, 2014, and shall terminate as set forth herein.

#### **1.0 Definitions**

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR 160.103, 164.105, 164.402, 164.501, 164.502, 164.520 and in the HITECH Act, Subtitle D. Those terms include but are not limited to: Breach, Data, Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Subcontractor, Unsecured Protected Health Information, and Use.

#### **Specific Definitions**

"Agency" means the Florida Department of Management Services (DMS), an executive agency of the State of Florida, and the Division of State Group Insurance (DSGI) with its principle place of business at 4050 Esplanade Way, Suite 215, Tallahassee, FL 32399-0950.

"Business Associate" means United Healthcare of Florida, Inc. with a place of business at 9009 Corporate Lake Drive, Tampa, FL 33634.

"Contract" means the document that contains the terms and conditions for any services to be provided by the Business Associate to the Covered Entity effective as of January 1, 2012 and terminating upon contract expiration.

"Covered Entity" means the State of Florida's Division of State Group Insurance (DSGI).

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at CFR Part 160 and Part 164.

"Individual" has the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

"Parties" mean collectively the Agency and the Business Associate. A "Party" means either the Agency or the Business Associate.

"Plans" means the insurance coverages offered through the Covered Entity, as authorized in section 110.123, Florida Statutes.

“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

“Protected Health Information” is defined in HIPAA at 45 CFR 160.103, and as used in this Agreement also refers to the term “Protected Health Information,” as defined in the HITECH Act.

“Secretary” means the Secretary of the U.S. Department of Health and Human Services or designee.

“Security Incident” means any event resulting in computer systems, networks, or data being accessed, viewed, manipulated, damaged, destroyed or made inaccessible by an unauthorized activity. See National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide," for more information.

## **Part I – Privacy Provisions**

### **2.0 Obligations and Activities of Business Associate**

#### **Business Associate Agrees to:**

- (a) Not use or further disclose Protected Health Information other than as permitted or required by sections 3.0, 5.0 and 6.0 of this Agreement, or as required by applicable federal laws or laws of the State.
- (b) Use appropriate safeguards, and comply with Subpart C 45 CFR 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health other than as provided for by this Agreement.
- (c) Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- (d) Report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including Breaches of unsecured Protected Health Information as required by 45 CFR 164.410 and any security Incident of which it becomes aware.
- (e) Ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (f) Provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations, to Protected Health Information in a designated record set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR 164.524.
- (g) Make any Amendment(s) to Protected Health Information in a designated record set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR 164.526, in a prompt and reasonable manner consistent with the HIPAA regulations, or take other measures as necessary to satisfy Covered Entity obligation(s) under 45 CFR 164.526.

- (h) Make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- (i) Document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- (j) At Covered Entity's or Individual's request, Business Associate agrees to provide to Individual or Covered Entity an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations. The Business Associate shall assist the Covered Entity in complying with the HIPAA regulations relating to the required Disclosure, Amendment or Accounting.
- (k) Business Associate certifies that it is in compliance with all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162; and the Annual Guidance as issued by the Secretary pursuant to the HITECH Act, sec. 13401. Business Associate further agrees to ensure that any agent, including a subcontractor, that conducts standard transactions on its behalf, agrees to comply with the EDI Standards and the Annual Guidance.
- (l) Business Associate agrees to determine the Minimum Necessary type and amount of Protected Health Information required to perform services and will comply with 45 CFR 164.502(b) and 164.514(d).

### **3.0 Permitted or Required Uses and Disclosures by Business Associate**

#### **General Use and Disclosure**

- (a) Except as expressly permitted in writing by DMS/DSGI, Business Associate shall not divulge, disclose, or communicate Protected Health Information to any third party for any purpose not in conformity with this Contract without prior written approval from the Covered Entity.
- (b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).
- (c) Business Associate may use and disclose Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).
- (d) Business Associate may use and/or disclose Protected Health Information for Business Associate's proper management and administration, provided that: (1) Business Associate obtains reasonable assurances from the person whom Protected Health Information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person; and (2) the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health information has been breached. Business Associate also may make disclosures that are required by law. The Business Associate's use of

Protected Health Information as described in this paragraph is subject to and limited as described in 45 CFR 164.504(e)(2) and (4).

- (e) Business Associate may create a Limited Data Set only as necessary and required for the purpose of performing its obligations and services for Covered Entity, provided that Business Associate complies with the provisions of this Agreement.

#### **4.0 Obligations of Covered Entity to Inform Business Associate of Covered Entity's Privacy Practices, and any Authorizations or Restrictions.**

- (a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.
- (b) Covered Entity shall provide Business Associate with any changes in, or revocation of, Authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

#### **5.0 Confidentiality Under State Law**

- (a) In addition to the HIPAA privacy requirements, Business Associate agrees to observe the confidentiality requirements of section 110.123(9), Florida Statutes. In general, the referenced statute provides that patient medical records and medical claim records of state employees, former state employees, and their covered dependents are confidential and exempt from the provisions of section 119.07(1), Florida Statutes, known as the public records law of the State of Florida. Any person who willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation, including those residing or existing internal and external to the DMS/DSGI computer system, commits an offense in violation of section 815.04, Florida Statutes.

Confidentiality requirements protect more than unlawful disclosure of documents. The confidentiality requirements protect the disclosure of all records and information of DMS/DSGI, in whatever form, including the copying or verbally relaying of confidential information.

- (b) Receipt of a Subpoena. If Business Associate is served with subpoena requiring the production of DMS/DSGI records or information, Business Associate shall immediately contact the Department of Management Services, Office of the General Counsel, (850) 487-1082.

A subpoena is an official summons issued by a court or an administrative tribunal, which requires the recipient to do one or more of the following:

1. Appear at a deposition to give sworn testimony, and may also require that certain records be brought to be examined as evidence.
2. Appear at a hearing or trial to give evidence as a witness, and may also require that certain records be brought to be examined as evidence.

3. Furnish certain records for examination, by mail or by hand-delivery.
- (c) Employees and Agents. Business Associate acknowledges that the confidentiality requirements herein apply to all its employees, agents and representatives and subcontractors. Business Associate assumes responsibility and liability for any damages or claims, including state and federal administrative proceedings and sanctions, against DMS/DSGI, including costs and attorneys' fees, resulting from the breach by Business Associate of the confidentiality requirements of this Agreement.

#### **6.0 Permissible Requests by Covered Entity**

- (a) Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA, the Privacy Rule, the HITECH Act and of the laws of the State of Florida, if done by Covered Entity.
- (b) Covered Entity shall not provide Business Associate with more Protected Health Information than that which is minimally necessary for Business Associate to provide the services and, where possible, Covered Entity shall provide any Protected Health Information needed by Business Associate to perform the services in the form of a Limited Data Set, in accordance with the HIPAA regulations.

#### **7.0 Termination**

- (a) Protected Health Information. Prior to the termination of this Agreement, the Business Associate shall destroy or return to the Covered Entity 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. If it is not feasible or impossible to return or destroy Protected Health Information, the Business Associate shall immediately inform the Covered Entity of that and the Parties shall cooperate in securing the destruction of Protected Health Information, or its return to the Covered Entity. Pending the destruction or return of the Protected Health Information to the Covered Entity, protections are extended to such information, in accordance with the termination provisions in this section.
- (b) Termination for Cause. Without limiting any other termination rights the Parties may have, upon Covered Entity's knowledge of a material breach by Business Associate of a provision under this Agreement, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. If the Agreement of Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, the Covered Entity shall have the right to immediately terminate the Agreement. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.
- (c) Effect of Termination. Within sixty calendar days after termination of the Agreement for any reason, or within such other time period as mutually agreed upon in writing by the Parties, Business Associate shall return to Covered Entity or destroy all Protected Health Information maintained by Business Associate in any form and shall retain no copies thereof. Business Associate also shall recover, and shall return or destroy within such time period, any Protected Health Information in the possession of its subcontractors or agents. Within fifteen calendar days after termination of the Agreement for any reason, Business Associate shall notify Covered Entity in writing as to whether Business Associate elects to return or destroy such Protected Health Information, or otherwise as set forth in this section 7.0(c). If Business Associate elects to destroy such Protected Health Information, it shall certify to

Covered Entity in writing when and that such Protected Health Information has been destroyed. If any subcontractors or agents of the Business Associate elect to destroy the Protected Health Information, Business Associate will require such subcontractors or agents to certify to Business Associate and to Covered Entity in writing when such Protected Health Information has been destroyed. If it is not feasible for Business Associate to return or destroy any of said Protected Health Information, Business Associate shall notify Covered Entity in writing that Business Associate has determined that it is not feasible to return or destroy the Protected Health Information and the specific reasons for such determination. Business Associate further agrees to extend any and all protections, limitations, and restrictions set forth in this Agreement to Business Associate's use or disclosure of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information not feasible. If it is not feasible for Business Associate to obtain, from a subcontractor or agent, any Protected Health Information in the possession of the subcontractor or agent, Business Associate shall provide a written explanation to Covered Entity and require the subcontractors and agents to agree to extend any and all protections, limitations, and restrictions set forth in this Agreement to the subcontractors' or agents' uses or disclosures of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information not feasible.

## **Part II – Security Addendum**

### **8.0 Security**

Business Associate and the Agency agree to also address herein the applicable requirements of the Security Rule, codified at 45 CFR Part 164, Subparts A and C, issued pursuant to the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS"), so that the Covered Entity may meet compliance obligations under HIPAA-AS, the Parties agree:

- (a) **Security of Electronic Protected Health Information.** Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information (as defined in 45 CFR 160.103) that Business Associate creates, receives, maintains, or transmits on behalf of the Plans consistent with the Security Rule.
- (b) **Reporting Security Incidents within five (5) business days of Discovery.** Business Associate will report to the Plans any security incident of which Business Associate becomes aware that is (i) a successful unauthorized access, use or disclosure of the Plans' Electronic Protected Health Information; or (ii) a successful major (1) modification or destruction of the Plans' Electronic Protected Health Information or (2) interference with system operations in an information system containing the Plans' Electronic Protected Health Information. Upon the Plans' request, Business Associate will report any incident of which Business Associate becomes aware that is a successful minor (1) modification or destruction of the Plans' Electronic Protected Health Information or (2) interference with system operations in an information system containing the Plans' Electronic Protected Health Information.
- (c) **Compliance Date.** The Business Associate certifies compliance with section 8.0 on or before the date on which its representative signs this Agreement as set forth in the signature blocks at the end of this document.

### **Part III - HITECH Reporting Requirements**

#### **9.0 HITECH**

In the event of any inconsistency or conflict between Part II and Part III, the more stringent provision shall apply.

#### **Applicability of HITECH and HIPAA Privacy Rule and Security Rule Provisions**

Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), also known as the Health Information Technology Economic and Clinical Health (HITECH) Act, requires a Business Associate that contracts with the Agency, a HIPAA covered entity, to comply with the provisions of the HIPAA Privacy and Security Rules (45 CFR 160 and 164).

- (a) Reporting. The Business Associate shall make a good faith effort to identify any use or disclosure of Protected Health Information not provided for in this Contract.
- (b) To Covered Entity. The Business Associate will report to the Covered Entity, within ten business days of discovery, any use or disclosure of Protected Health Information not provided for in this Contract of which the Business Associate is aware. The Business Associate will report to the Covered Entity, within two (2) business days of discovery, any Security Incident of which the Business Associate is aware. The day the breach is discovered will be considered the first business day of the incident reporting period. A violation of this paragraph shall be a material violation of this Contract. Such notice shall include the identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach.
- (c) To Individuals. In the case of a breach of Protected Health Information, as defined by HIPAA and HITECH, by the Business Associate, the Business Associate shall first notify the Covered Entity of the pertinent details of the breach and upon prior approval of the Covered Entity shall notify each individual whose unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired or disclosed as a result of such breach. Such notification shall be in writing by first-class mail to the individual or personal representative (or the next of kin if the individual is deceased) at the last known address of the individual or next of kin or personal representative, respectively, or, if specified as a preference by the individual, by electronic mail. Where there is insufficient, or out-of-date contract information (including a phone number, email address, or any other form of appropriate communication) that precludes written (or, if specifically requested, electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting on the web site of the covered entity involved or notice in major print or broadcast media, including major media in the geographic areas where the individuals affected by the breach likely reside. In any case deemed by the Business Associate to require urgency because of possible imminent misuse of unsecured Protected Health Information, the Business Associate may also provide information to individuals by telephone or other means, as appropriate.
- (d) To Media. In the case of a breach of Protected Health Information discovered by the Business Associate where the unsecured Protected Health Information of more than 500 persons is reasonably believed to have been, accessed, acquired, or disclosed, after prior approval by the Covered Entity, the

Business Associate shall provide notice to prominent media outlets serving the State or relevant portion of the State involved.

- (e) To Secretary of Health and Human Services. The Business Associate shall cooperate with the Covered Entity to provide notice to the Secretary of Health and Human Services of unsecured Protected Health Information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals, such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the Business Associate may maintain a log of such breach occurring and annually submit such log to the Covered Entity so that it may satisfy its obligation to notify the Secretary of Health and Human Services documenting such breaches occurring in the year involved.
- (f) Content of Notices. All notices required under this Attachment shall include the content set forth in the regulations implementing section 13402(f), Title XIII of the American Recovery and Reinvestment Act of 2009, except that references therein to a "covered entity" shall be read as references to the Business Associate.
- (g) Financial Responsibility. The Business Associate shall be responsible for reasonable costs related to the notices required under this Attachment.
- (h) Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of Protected Health Information in violation of this Attachment.

#### **Part IV**

#### **10.0 Miscellaneous**

- (a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule, the Security Rule or the HITECH Act means the section as in effect or as amended, and for which compliance is required.
- (b) Amendment. Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, Standard Transactions, the security of Health Information, or other aspects of HIPAA-AS or the HITECH Act applicable or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either Party may, by written notice to the other Party, amend this Agreement in such manner as such Party determines necessary to comply with such law or regulation. If the other Party disagrees with such Amendment, it shall notify the first Party in writing within thirty calendar days' notice. If the Parties are unable to agree on an Amendment within thirty calendar days thereafter, then either of the Parties may terminate the Agreement on thirty calendar days written notice to the other Party.
- (c) Survival. The respective rights and obligations of Business Associate under Section 7.0 of this Agreement shall survive the termination of this Agreement.
- (d) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule and the confidentiality requirements of the State of Florida, including section 110.123(9), Florida Statutes.
- (e) No third party beneficiary. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assignees of the

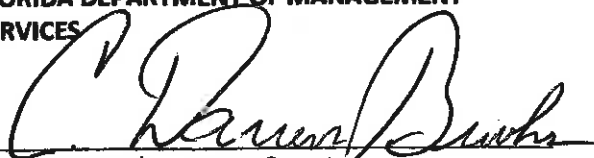


Parties, any rights, remedies, obligations, or liabilities whatsoever.

- (f) Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Florida to the extent not preempted by the Privacy Rules or other applicable federal law.
- (g) The laws of the State of Florida shall apply to the interpretation of this Agreement or in case of any disagreement between the Parties; the venue of any proceedings shall be the appropriate federal or state court in Leon County, Florida.
- (h) Indemnification and performance guarantees. Business Associate shall indemnify, defend, and save harmless the State of Florida and individuals covered by the Plans for any financial loss as a result of the claims brought by third parties and which are caused by the failure of Business Associate, its officers, directors or agents to comply with the terms of this Agreement.
- (i) Independent Contractors. Business Associate and Covered Entity are independent contractors and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise, or agency between Business Associate and Covered Entity. Neither Business Associate nor Covered Entity will have the power to bind the other or incur obligations on the other Party's behalf without the other Party's prior written consent, except as otherwise expressly provided in this Agreement.
- (j) Conflicts. In the event that any terms of this Agreement are inconsistent with the terms of the Underlying Agreement, then the terms of this Agreement shall control.

Business Associate shall not assign either its obligations or benefits under this Agreement without the expressed written consent of the Covered Entity, which shall be at the sole discretion of the Covered Entity. Given the nature of this Agreement, neither subcontracting nor assignment by the Business Associate is anticipated and the use of those terms herein does not indicate permission to assign or subcontract has been granted.

**FLORIDA DEPARTMENT OF MANAGEMENT  
SERVICES**

  
C. Darren Brooks, Deputy Secretary

10/15/14  
Date

**UNITED HEALTHCARE OF FLORIDA, INC.**

  
Signature

Dan Rocha Regional Contract Manager  
Print Name and Title

9/22/2014  
Date

**Attachment D: Affidavit of Best Pricing**

Regarding the Contract between  
United Healthcare of Florida, Inc. (the "Service Provider")  
And  
State of Florida, Department of Management Services  
Contract No.: DMS 10/11-011  
Effective January 1, 2015

Pursuant to Section 4(b) of Form PUR 1000 of the Contract, the undersigned Service Provider hereby attests that the Service Provider is in compliance with the Best-Pricing clause in the Contract.

**Service Provider Name:** United Healthcare of Florida, Inc.

**Service Provider's Federal Employer Identification Number (FEIN #):** \_\_\_\_\_

**Authorized Signature:** \_\_\_\_\_

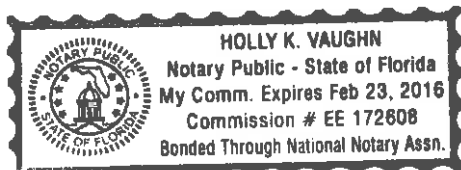
**Print Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_

Sworn to (or affirmed) and subscribed before me on this

7<sup>th</sup> day of October by



\_\_\_\_\_  
Holly K. Vaughn

(Signature of Notary)

Check One:

☒ Personally Known

☐ Produced the following ID \_\_\_\_\_

**Attachment E: Affidavit of No Off-shoring of Data**

Regarding the Contract between  
United Healthcare of Florida, Inc. (the "Service Provider")  
And  
State of Florida, Department of Management Services  
Contract No.: DMS 10/11-011  
Effective upon execution

Pursuant to Section 3.3.6 of the Contract, the undersigned Service Provider hereby attests that the Service Provider does not utilize offshore Subcontractors who have access to or otherwise can transmit sensitive or confidential member data in any form and that the Service Provider is in compliance with the Subcontractor section in the Contract.

**Service Provider's Name:** United Healthcare of Florida, Inc.

**Service Provider's Federal Employer Identification Number (FEIN #):** \_\_\_\_\_

**Authorized Signature:** \_\_\_\_\_

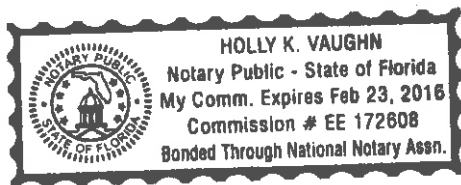
**Print Name:** F. Benson Parker, Jr.

**Title:** Vice President

**Date:** 10/7/14

Sworn to (or affirmed) and subscribed before me on this

7<sup>th</sup> day of October by \_\_\_\_\_  
Holly K. Vaughn  
(Signature of Notary)



Check One:

☒ Personally Known

☐ Produced the following ID \_\_\_\_\_

### **Attachment F: No Off-shoring of Data**

Service Provider's Responsibility to Notify Department.

Notwithstanding any provision of this Contract to the contrary, the Service Provider shall notify the Department as soon as possible and in all events within one (1) business day in the event it discovers any State of Florida sensitive or confidential member data (Data) is breached, any unauthorized access of Data occurs (even by persons or companies with authorized access for other purposes), any unauthorized transmission of Data, or any credible allegation or suspicion of a material violation of the above. This notification is required whether the event affects one plan participant or the entire population. The notification shall be clear and conspicuous and include a description of the following:

- a) The incident in general terms.
- b) The type of Data that was subject to the unauthorized access and acquisition.
- c) The number of individuals who were, or potentially have been, affected by the breach.
- d) The actions taken by the Service Provider to protect the Data from further unauthorized access. However, the description of those actions in the written notice may be general so as not to further increase the risk or severity of the breach.

**Attachment G: Summary Plan Description**

**Effective January 1, 2015**