[Home and Community Based Services][Long Term Services and Supports]
Provider Agreement

UnitedHealthcare Insurance Company is entering into this agreement with you, [*provider name*]. It is doing so on behalf of itself, UnitedHealthcare of Ohio, Inc., UnitedHealthcare Community Plan of Ohio, Inc. and its other affiliates (collectively referred to as "United") for certain products and services we offer our customers, all of which we describe in the attached Appendix 2

This agreement applies to you and the services you provide in all of your practice arrangements and for all of your tax identification numbers.

What you will do

You need to be credentialed in accordance with our credentialing plan for [Home and Community Based Services][Long Term Services and Supports] providers for the duration of this agreement.

Within one year of the effective date of this agreement, we expect that you conduct business with us on an electronic basis to the extent that we are able to conduct business electronically (described in the Administrative Guide), including but not limited to determining whether your patient is currently a customer, verifying the customer's benefit, and submitting your claim. We will communicate enhancements at www.UHCprovider.com as they become available and will make information available to you as to which products are supported by www.UHCprovider.com.

You must submit your claims for reimbursement (whether by claim form, invoice or other method, as set forth in this agreement) within 90[120][150][180] days of the date of service. After we receive your claim, if we request additional information in order to process your claim, you must submit this additional information within 90 days of our request. If your claim or the additional information is not submitted within these timeframes, you will not be reimbursed for the services, and you may not charge our customer.

You will submit claims only for services performed by you or your staff. Pass through billing is not payable under this agreement and may not be billed to our customer.

You will submit claims that supply all applicable information. These claims are complete claims. Further information about complete claims is provided in our Administrative Guide.

If you disagree with our payment determination on a claim, you may submit an appeal as described in our Administrative Guide.

You will not charge our customers anything for the services you provide, if those services are covered services under their benefit contract, but the applicable co-pay, coinsurance or deductible amount. If the services you provide are denied or otherwise not paid due to your failure to notify us, to file a timely claim, to submit a complete claim, to respond to our request for information, or based on our reimbursement policies and methodologies, you may not charge our customer. If you collect payment from, bring a collection action against, or assert a lien against a customer for covered services rendered (other than for the applicable co-payment, deductible or coinsurance), you will be in breach of this agreement and we may deduct, from any amounts otherwise due you, the amount wrongfully collected from customers, and may also deduct an amount equal to any costs or expenses incurred by us, or the customer.

If the services you provide are not covered under our customer's benefit contract, you may only bill our customer directly if that is permissible under 42 CFR Section 447.15, as well as state laws, regulations and the applicable state Medicaid contract.

You will cooperate with our reasonable requests to provide information that we need and obtain customer consent required to authorize you to provide access to required information. We may need this information to perform our obligations under this agreement, under our programs and agreements with our customers, or as required by regulatory or accreditation agencies.

You will refer customers only to other network physicians and providers, except as permitted under our customer's benefit contract, or as otherwise authorized by us.

You will hold all applicable registrations, permits, licenses, and other approvals and consents required under applicable law in order to perform your obligations under this agreement and will comply with all applicable regulatory requirements, including but not limited to those relating to confidentiality of customer medical information.

In the event you are acquired by, merged with, or otherwise become affiliated with another provider of health care services that is already under contract with us or one of our affiliates to participate in our network of health care providers, this agreement and the other agreement will each remain in effect and will continue to apply as they did prior to the acquisition, merger or affiliation, unless otherwise agreed to in writing by all parties to those agreements.

If you decide to transfer some or all of your assets to another entity, and the result of the transfer would be that all or some of the services subject to this agreement would be rendered by the other entity rather than by you, you must first request that we approve an assignment of this agreement as it relates to those services and the other entity must agree to assume this agreement.

You will ensure that anyone rendering services in connection with this agreement adheres to the requirements of this agreement. You are solely responsible for all services rendered in connection with this agreement.

To the extent applicable, during the term of this agreement, you will maintain and will require your subcontractors to maintain, at your (or your subcontractor's) sole cost and expense:

a) commercial general liability insurance and/or umbrella liability insurance, in the amount of [$1,000,000] per occurrence and [$3,000,000] aggregate; and
b) coverage for [medical malpractice and/or] professional liability insurance, in the amount of [$1,000,000] per occurrence and [$2,000,000] in aggregate.

In addition, you attest that you maintain, and at all times during the term of this agreement will continue to maintain, at your sole cost and expense: (i) workers' compensation and/or employer's liability insurance to the full extent required by applicable state law; and, (ii) if transportation services are provided as part of this agreement, business automobile liability insurance to the full extent required by applicable state law.

Our approval or acceptance of your insurance does not, in any way, represent that such insurance is sufficient or adequate to protect your interests or liabilities and such insurance coverage will be considered the minimum acceptable coverage.

Upon written request, you will submit to us, in writing, evidence of insurance coverage. You will give us ten (10) days written notice in the event of any termination, cancellation or material change in your

insurance.

You will also give notice to us within ten (10) days after any event that causes you to be out of compliance with licensure, or of any change in your name or Taxpayer Identification Number. In addition, you will give us forty-five (45) days prior written notice of changes in existing remit address(es) and other demographic information.

You acknowledge that you have been given the opportunity to review, and will cooperate with, our protocols which will be made available to you online or upon request. Some or all protocols also may be disseminated in the form of an Administrative Guide, or in other communications. We may change the protocols from time to time and will use reasonable commercial efforts to inform you at least thirty (30) days in advance of any material changes.

What we will do

We or the other applicable participating entity will promptly adjudicate and pay your complete claim for services covered by our customer's benefit contract. If you submit claims that are not complete,

- You may be asked for additional information so that your claim may be adjudicated; or
- Your claim may be denied and you will be notified of the denial and the reason for it; or
- We may, in our discretion, attempt to complete the claim and have it paid by us or the other applicable participating entity based on the information that you gave in addition to the information we have.

If governing law requires us to pay interest or another penalty for a failure to pay your complete claim for covered services within a certain time frame, we will follow those requirements. The interest or other penalty required by law will be the only additional obligation for not satisfying a payment obligation to you in a timely manner. In addition, if we completed a claim of yours that was not complete, there shall be no interest or other late payment obligation to you even if we subsequently adjust the payment amount based on additional information that you provide.

If either of us believes that a claim has not been paid correctly, either of us may seek correction of the payment within a 12-month period following the date the claim was paid, except that overpayments as a result of abusive or fraudulent billing practices may be pursued by us beyond the 12-month time frame mentioned above. In the event of an overpayment, we will correct these errors by adjusting future claim payment and/or by billing you for the amount of the overpayment.

How long our agreement lasts; how it gets amended; and how it can end

Assuming you are credentialed by us, and we execute this agreement, you will receive a copy from us with the effective date noted below the signature block. It continues until one of us terminates it, as described below.

We can amend this agreement or any of the appendices on ninety (90) days written or electronic notice by sending you a copy of the amendment, unless shorter notice is necessary in order to meet regulatory compliance. Your signature is not required to make the amendment effective. However, if you do not wish to continue your participation with our network as changed by an amendment that is not required by law or regulation but that includes a material adverse change to this agreement, then you may terminate this agreement on [sixty (60)][ninety (90)] days written notice to us so long as you send this termination

notice within thirty (30) days of your receipt of the amendment.

In addition, either you or we can terminate this agreement, effective on an anniversary of the date this agreement begins, by providing at least [ninety (90)][sixty (60)] days prior written notice. Either you or we can terminate this agreement at any time if the other party has materially breached this agreement, by providing sixty (60) days written notice, except that if the breach is cured before our agreement ends, the agreement will continue.

Either of us can immediately terminate this agreement if the other becomes insolvent or has bankruptcy proceedings initiated.

Finally, we can immediately terminate this agreement for the following reasons: (1) if we become aware of any criminal charge related to your services or an indictment, arrest, or conviction for a felony; (2) your failure to meet our credentialing program requirements to the extent that those requirements apply to you; (3) if any governmental agency or authority (including Medicare or Medicaid) sanctions you; or (4) if you lose applicable accreditation, licensure, permit or other approval required to provide services under this agreement.

We both agree that termination notices under this agreement must be sent by certified mail, return receipt requested, to [*UHC Mailing Address*], or to the post office address you provided to us. We both will treat termination notices as "received" on the third business day after they are sent.

About data and confidentiality

We agree that your medical records do not belong to us. You agree the information contained in the claims you submit is ours. We both will protect the confidentiality of our customers' information in accordance with applicable state and federal laws, rules, and regulations.

SUBSTITUTE LANGUAGE: when contracting with LTSS providers (as indicated by selection of the title "Long Term Services and Supports Provider Agreement":
In accordance with certain provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, you are deemed a Business Associate of ours. We both agree to abide by the Business Associate Agreement and Security Appendix attached hereto and incorporated herein by reference. We both will protect the confidentiality of our customers' information in accordance with applicable state and federal laws, rules, and regulations.

We are both prohibited from disclosing to third parties any fee schedule or rate information. There are three exceptions:

- You can disclose to our customer information relating to our payment methodology for a service the customer is considering (e.g., global fee, fee for service), but not specific rates (unless for purposes of benefit administration).

- We and the participating entities may use this information to administer our customers' benefit contracts and to pay your claims. We also may permit access to information by auditors and other consultants who need the information to perform their duties, subject to a confidentiality agreement.

- We both may produce this information in response to a court order, subpoena or regulatory requirement to do so, provided that we use reasonable efforts to seek to maintain confidential

treatment for the information, or to a third party for an appropriate business purpose, provided that the disclosure is pursuant to a confidentiality agreement and the recipient of the disclosure is not a competitor of either of us.

What if we do not agree

The parties will work together in good faith to resolve any and all disputes between them ("Disputes") following the dispute procedures set out in our Administrative Guide. Disputes may include, but are not limited to the existence, validity, scope or termination of this agreement or any term thereof, and all questions of arbitrability, with the exception of any question regarding the availability of class arbitration or consolidated arbitration, which is expressly waived below. Disputes also include any dispute in which you are acting as the assignee of one or more customer. In such cases, these procedures will apply, including, without limitation, the requirement for arbitration.

If the Dispute pertains to a matter which is generally administered by certain United procedures, such as a credentialing or quality improvement plan, the policies and procedures set forth in that plan must be fully exhausted by you before you may invoke any right to arbitration under this section.

For Disputes regarding payment of claims, a party must have timely initiated and completed the claim reconsideration and appeal process as set forth in the Administrative Guide in order to initiate the Dispute process.

If the parties are unable to resolve any Dispute within 60 days after notice, either party may submit the Dispute to binding arbitration conducted by the American Arbitration Association ("AAA"). The arbitrators will use the AAA Healthcare Payor Provider Arbitration Rules, as amended. However, if a case involves a Dispute in which a party seeks an award of $1,000,000 or greater or seeks termination of this agreement, a panel of three arbitrators will be used. The arbitrator(s) will be selected from the AAA National Healthcare Roster or the AAA's National Roster of Arbitrators. Unless otherwise agreed in writing, arbitration must be initiated within one year after the date on which written notice of the Dispute was given, or any appeal process described in the Administrative Guide, whichever is later. If arbitration is not initiated in that time frame, the right to pursue the Dispute in any forum is waived.

Any arbitration proceeding under this agreement will be conducted in [*name of county*] County, [*state*]. The arbitrator(s) may construe or interpret but must not vary or ignore the terms of this agreement and will be bound by controlling law. The arbitrator(s) have no authority to award punitive, exemplary, indirect or special damages, except in connection with a statutory claim that explicitly provides for that relief.

Except as may be required by law, neither a party, including without limitation, the parties' representatives, consultants and counsel of record in the arbitration, nor an arbitrator may disclose the existence, content, or results of any arbitration hereunder, or any Confidential Arbitration Information without the prior written consent of all parties. "Confidential Arbitration Information" means any written submissions in an arbitration by either party, discovery exchanged, evidence submitted, transcriptions or other records of hearings in the matter and any orders and awards issued, and any reference to whether either party won, lost, prevailed, or did not prevail against the other party in any arbitration proceeding, as well as any settlement agreement related to an arbitration. However, judgment on the award may be entered under seal in any court having jurisdiction thereof, by either party.

The parties expressly intend that any arbitration be conducted on an individual basis, so that no third parties may be consolidated or joined or allowed to proceed with class arbitration. The parties agree that

any arbitration ruling allowing class arbitration, or requiring consolidated arbitration involving any third party(ies), would be contrary to the terms of this agreement and require immediate judicial review. Notwithstanding anything in this agreement to the contrary, this paragraph may not be severed from this provision of the agreement under any circumstances, including but not limited to unlawfulness, invalidity or unenforceability.

The decision of the arbitrator(s) on the points in dispute will be binding. The parties acknowledge that because this agreement affects interstate commerce, the Federal Arbitration Act applies. In the event any court determines that this arbitration procedure is not binding or otherwise allows litigation involving a Dispute to proceed, the parties hereby waive any and all right to trial by jury in, or with respect to, the litigation. The litigation would instead proceed with the judge as the finder of fact.

In the event a party wishes to terminate this agreement based on an assertion of uncured material breach, and the other party disputes whether grounds for termination exist, the matter will be resolved through arbitration under this provision. While the arbitration remains pending, the termination for breach will not take effect.

This provision will survive any termination of this agreement.

What is our relationship to one another

You are an independent contractor. This means we do not have an employer-employee, principal-agent, partnership, joint venture, or similar arrangement.

We may assign this agreement to any entity that is an affiliate of ours at the time of the assignment.

This is it

This contract, the appendices and the items referenced in the attached Appendix 1, constitute our entire understanding. It replaces any other agreements or understandings with regard to the same subject matter -- oral or written -- that you have with us or any of our affiliates.

Federal law and the applicable law of the jurisdiction where you provide health care services govern our agreement. Such laws and the rules and regulations promulgated under them, when they are applicable, control and supersede our agreement. The Regulatory Appendix referenced in Appendix 1, and any attachment to it, is expressly incorporated to govern our agreement and is binding on both of us. In the event of any inconsistent or contrary language between the Regulatory Appendix (when it applies) and any other part of our agreement, including but not limited to appendices, amendments and exhibits, the Regulatory Appendix will control.

Conclusion

If you agree with these terms, please execute both copies of the agreement below and return them to us. With your signature, you confirm you understand the contract, including the dispute resolution procedures described in the section of this agreement entitled "What if we do not agree", the appendices and the items referenced in the attached Appendix 1.

THIS AGREEMENT CONTAINS A BINDING ARBITRATION PROVISION THAT MAY BE ENFORCED BY THE PARTIES.

AGREED BY:

[PROVIDER]

Address to be used for giving notice under the agreement:

Signature: _____

Print Name: _____

DBA (if applicable): _____

Date: _____

Email: _____

Street: _____

City: _____

State: _____

Zip Code: _____

TIN: _____

National Provider Identification (NPI) Number: _____

UnitedHealthcare Insurance Company contracting on behalf of itself, UnitedHealthcare of Ohio, Inc., UnitedHealthcare Community Plan of Ohio, Inc. and its other affiliates, as signed by its authorized representative:

Signature _____

Print Name _____

Date _____

For office use only:

Month, day and year in which agreement is first effective: ___ ___ / ___ ___ / ___ ___

Appendix 1

We include as part of our agreement the following additional materials that bind you and us:

Appendix 2	**Definitions, Products and Services** This appendix sets forth definitions for our "customer" and "participating entities" as well as lists the type of benefit contracts offered to our customers.
[Payment Appendix(ices)	Fee Information Document. This document sets forth the fees that will be paid for your services.]
Appendix 3	Locations. This document provides information about your office, billing, and mailing locations. Please remember that, as described on page 2, this agreement applies to all of your locations even if you do not list all of your current locations or if you add a location in the future.
State Regulatory Requirements Appendix	In some instances, states add requirements to our agreement that are set forth in this appendix.
Medicaid and/or CHIP Regulatory Requirements Appendix(ices)	(These appendix(ices) apply only if you are in our Medicaid and/or CHIP network). Your participation in our network for customers with Medicaid or CHIP benefit contracts is subject to additional requirements set forth in this appendix.
Medicare Regulatory Requirements Appendix	(This appendix applies only if you are in our Medicare network.) Your participation in our network for customers with Medicare benefit contracts is subject to additional Medicare requirements set forth in this appendix.
[Services Addendum	This addendum sets forth the services that you will provide.]
[Business Associate Agreement	The BAA sets forth obligations under HIPAA, as applicable.]
[Security Appendix	This appendix sets forth electronic data exchange requirements.]

<table>
<tr><td>Administrative Guide</td><td>
This guide governs the mechanics of our relationship. Our Administrative Guide may be viewed by going to www.UHCprovider.com. We may make changes to the Administrative Guide or other administrative protocols upon 30 days electronic or written notice to you.

For services rendered to customers enrolled in certain benefit contracts that may be included under this agreement, you will be subject to additional requirements described in or made available to you through one or more additional provider manuals (“Additional Manuals”). When this agreement refers to protocols or reimbursement policies it is also referring to the Additional Manuals. The Additional Manuals will be made available to you on a designated website or upon request.

In the event of any conflict between this agreement or the “UnitedHealthcare Care Provider Administrative Guide” or other UnitedHealthcare protocols and reimbursement policies, and any Additional Manual, in connection with any matter pertaining to customers enrolled in the benefit contracts to which the Additional Manual applies, that Additional Manual will govern, unless statutes and regulations dictate otherwise. We may make changes to the protocols and reimbursement policies subject to this Appendix in accordance with the provisions of the agreement relating to protocols and reimbursement policy changes.

The benefit contracts, names of the Additional Manuals, and name of the website to view and download the manuals, when applicable, are set forth in the table below. We will notify you of any changes in the location of the Additional Manuals. You may request a copy of the Additional Manual.

Table 1.
<table>
<tr><th>Benefit Contract</th><th>Description of Applicable Additional Manual</th><th>Website</th></tr>
<tr><td>[Ohio Medicaid Benefit Contracts</td><td>UnitedHealthcare Community Plan of Ohio Physician, Health Care Professional, Facility and Ancillary Provider Care Provider Manual: Medicaid</td><td>www.UHCprovider.com]</td></tr>
<tr><td>[Ohio Medicare and Medicaid Enrollees Benefit Plans</td><td>UnitedHealthcare Community Plan of Ohio Physician, Health Care Professional, Facility and Ancillary Provider Care Provider Manual: UnitedHealthcare Connected for MyCare Ohio</td><td>www.UHCprovider.com]</td></tr>
</table>
</td></tr>
</table>

Appendix 2
Definitions, Products and Services

1. Customer. Individuals who are enrolled in benefit contracts insured or administered by us or any participating entity are included in our use of the phrase "customer" in this agreement.

2. Participating entities. The following entities have access to our agreement:

- UnitedHealthcare Insurance Company and its affiliates;
- Groups receiving administrative services from UnitedHealthcare Insurance Company or its affiliates or that have arranged for network access through an entity that has contracted with UnitedHealthcare Insurance Company or one of its affiliates.

3. Products and services.

You will participate in networks where our customers are enrolled in benefit contracts of the types generally described below.

- [Ohio Medicaid Benefit Contracts.]

- [Medicare Advantage Benefit Contracts.]

- [Ohio Medicare and Medicaid Enrollees (MME) Benefit Contracts.]

This agreement does not apply to benefit contracts other than those described above.

4. Definitions.

Note: We may adopt a different name for a particular benefit contract, and/or may modify information referenced in the definitions in this Appendix 2 regarding customer identification cards. If that happens, this Appendix 2 will continue to apply to those benefit contracts as it did previously, and we will provide you with the updated information. Additionally, we may revise the definitions in this Appendix 2 to reflect changes in the names or roles of our business units, provided that doing so does not change your participation status in benefit contracts impacted by that change, and further provided that we provide you with the updated information.

- Medicaid Benefit Contracts means benefit contracts that offer coverage to beneficiaries of a program authorized by Title XIX of the federal Social Security Act, and jointly financed by the federal and state governments and administered by the state.

- Children's Health Insurance Program ("CHIP") Benefit Contracts means benefit contracts under the program authorized by Title XXI of the federal Social Security Act that are jointly financed by the federal and state governments and administered by the state.

- [Medicare Advantage Benefit Contracts means benefit contracts sponsored, issued or administered by a Medicare Advantage organization as part of:
  i) the Medicare Advantage program under Title XVIII, Part C of the Social Security Act, or
  ii) the Medicare Advantage program together with the Prescription Drug program under Title XVIII, Part C and Part D, respectively, of the Social Security Act,
  as those program names may change from time to time.]

- [Medicare and Medicaid Enrollees (MME) Benefit Contracts means the CMS sponsored Financial Alignment Demonstration Plan providing integrated care benefits for individuals eligible for both the state Medicaid program and the Medicare program (Parts A, B, C and D). At such time as this benefit contract is no longer a demonstration project and is fully implemented in the state, this definition will be interpreted to refer to the fully implemented plan.]

Appendix 3 - LOCATIONS

NOTE: Please attach additional copies of this page if you need to list additional locations.

Please remember that, as described on page 2, this agreement applies to all of your locations even if you do not list all of your current locations or if you add a location in the future.

Provider:

Primary Service Location Address:	Address:		
	City:	State:	Zip:
	Tel #:	Fax #:	
Billing Address:	Address:		
	City:	State:	Zip:
	Tel #:	Fax #:	

Additional Service Location Address:	Address:		
	City:	State:	Zip:
	Tel #:	Fax #:	
Billing Address: ❑ Same as above	Address:		
	City:	State:	Zip:
	Tel #:	Fax #:	

Mailing Address:	Address:		
	City:	State:	Zip:
	Tel #:	Fax #:	

[BUSINESS ASSOCIATE AGREEMENT

The parties hereby agree as follows:

1. DEFINITIONS

1.1 All capitalized terms used in this Appendix not otherwise defined in this Appendix have the meanings established in either the Agreement or for purposes of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended and supplemented by HITECH, as each is amended from time to time (collectively, "HIPAA"). To the extent a term is defined in both the Agreement and in this Appendix or in HIPAA, the definition in this Appendix or in HIPAA shall govern.

1.2 "Affiliate" shall have the meaning ascribed to it in the Agreement. If the term "Affiliate" is not defined in the Agreement, then "Affiliate" shall mean, for purposes of this Appendix, any subsidiary of UnitedHealth Group Inc.

1.3 "Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exclusions set forth, in 45 C.F.R. § 164.402.

1.4 "Breach Rule" means the federal breach regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Part 164 (Subpart D).

1.5 "Compliance Date" means the later of September 23, 2013 or the effective date of the Agreement.

1.6 "Electronic Protected Health Information" or "ePHI" means PHI that is transmitted or maintained in Electronic Media.

1.7 "GLBA" means the Gramm-Leach-Bliley Act and all associated existing and future implementing regulations, when and as each is effective.

1.8 "HITECH" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all associated existing and future implementing regulations, when and as each is effective.

1.9 "NPI" means Nonpublic Personal Information, as defined in 16 C.F.R. § 313.3.

1.10 "PHI" means Protected Health Information, as defined in 45 C.F.R. § 160.103, and is limited to the Protected Health Information received from, or received, maintained, created or transmitted on behalf of, United (for itself and/or applicable Covered Entity customers) by Provider in performance of the Services.

1.11 "Privacy Rule" means the federal privacy regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Parts 160 and 164 (Subparts A & E).

1.12 "Provider" means you, the party named in the Agreement.

1.13 "Security Rule" means the federal security regulations, as amended from time to time, issued pursuant to HIPAA and codified at 45 C.F.R. Parts 160 and 164 (Subparts A & C).

1.14 "Services" as used in this Appendix, means, to the extent and only to the extent they involve the receipt, creation, maintenance, transmission, use or disclosure of PHI, the services provided by Provider to United as set forth in the Agreement.

2. RESPONSIBILITIES OF PROVIDER. With regard to its use and/or disclosure of PHI, Provider agrees to:

2.1 not use and/or further disclose PHI except as necessary to provide the Services, as permitted or required by this Appendix, and in compliance with each applicable requirement of 45 C.F.R. § 164.504(e), or as otherwise Required by Law; provided that, to the extent Provider is to carry out a Covered Entity's obligations under the Privacy Rule, Provider will comply with the requirements of the Privacy Rule that apply to that Covered Entity in the performance of those obligations.

2.2 implement and use appropriate administrative, physical and technical safeguards and, as of the Compliance Date, comply with applicable Security Rule requirements with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this Appendix, including at a minimum, but in any event not limited to, any safeguards set forth in the Agreement or other applicable contracts or agreements between the parties. For the avoidance of doubt, the requirements set forth in the Agreement or other applicable contracts or agreements between the parties do not limit in any way whatsoever Provider's obligations under this Section 2.2 to comply with applicable Security Rule requirements.

2.3 without unreasonable delay, and in any event on or before forty-eight (48) hours after its discovery by Provider, report to United in writing: (i) any use or disclosure of PHI not provided for by this Appendix of which it becomes aware in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(C); and/or (ii) any Security Incident of which Provider becomes aware in accordance with 45 C.F.R. § 164.314(a)(2)(i)(C).

2.4 without unreasonable delay, and in any event on or before forty-eight (48) hours after its Discovery by Provider, notify United of any incident that involves an unauthorized acquisition, access, use or disclosure of PHI, even if Provider believes the incident will not rise to the level of a Breach. The notification shall include, to the extent possible, and shall be supplemented on an ongoing basis with: (i) the identification of all individuals whose Unsecured PHI was or is believed to have been involved; (ii) all other information required for or requested by United (or the applicable Covered Entity) to perform a risk assessment in accordance with 45 C.F.R. § 164.402 with respect to the incident to determine whether a Breach of Unsecured PHI occurred; and (iii) all other information reasonably necessary to provide notice to the applicable Covered Entities individuals, HHS and/or the media, all in accordance with the Breach Rule. Notwithstanding the foregoing, in United's sole discretion and in accordance with its directions, and without limiting in any way any other remedy available to United at law, equity or contract, including but not limited to any rights or remedies the United may have under the Agreement, Provider (i) shall conduct, or pay the costs of conducting, an investigation of any incident required to be reported under this Section 2.4, (ii) shall reimburse and pay United for all expenses and costs incurred by United that arise from an investigation of any incident required to be reported under this Section 2.4 and (iii) shall provide, and/or pay the costs of providing, the required notices as set forth in this Section 2.4.

2.5 in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), ensure that any subcontractors of Provider that create, receive, maintain or transmit PHI on behalf of Provider agree, in writing, to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Provider with respect to that PHI, including complying with the applicable Security Rule requirements with respect to ePHI; provided that, in any event Provider shall require its subcontractors (and shall require those subcontractors to require their subcontractors) to report to Provider any use or disclosure of PHI or Security Incident required to be reported under Sections 2.3 and 2.4 on or before forty-eight (48) hours after its discovery by any of those subcontractors.

2.6 make available its internal practices, books and records relating to the use and disclosure of PHI to the Secretary for purposes of determining the applicable Covered Entity's compliance with the Privacy Rule.

2.7 document, and within thirty (30) days after receiving a written request from United, make available to United information necessary for United or its applicable Covered Entity customer to make an accounting of disclosures of PHI about an Individual or, when and as requested by United, make that information available directly to an Individual, all in accordance with 45 C.F.R. § 164.528 and, as of the

later of the date compliance is required by final regulations or the effective date of the Agreement, 42 U.S.C. § 17935(c).

2.8 provide access to United, within fifteen (15) days after receiving a written request from United, to PHI in a Designated Record Set about an Individual, or when and as requested by United, provide that access directly to an Individual, all in accordance with the requirements of 45 C.F.R. § 164.524, including as of the Compliance Date, providing or sending a copy to a designated third party and providing or sending a copy in electronic format in accordance with 45 C.F.R. § 164.524.

2.9 to the extent that the PHI in Provider's possession constitutes a Designated Record Set, make available, within thirty (30) days after a written request by United, PHI for amendment and incorporate any amendments to the PHI as requested by United, all in accordance with 45 C.F.R. § 164.526.

2.10 accommodate reasonable requests for confidential communications in accordance with 45 C.F.R. § 164.522(b), as requested by United or as directed by the Individual to whom the PHI relates.

2.11 notify United in writing within three (3) days after Provider's receipt directly from an Individual of any request for an accounting of disclosures, access to or amendment of PHI or for confidential communications as contemplated in Sections 2.7-2.10.

2.12 request, use and/or disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure; provided, that Provider shall comply with 45 C.F.R. §§ 164.502(b) and 164.514(d) as of the Compliance Date.

2.13 not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 45 C.F.R. § 164.502(a)(5)(ii) as of the Compliance Date.

2.14 not make or cause to be made any communication about a product or service that is prohibited by 45 C.F.R. §§ 164.501 and 164.508(a)(3) as of the Compliance Date.

2.15 not make or cause to be made any written fundraising communication that is prohibited by 45 C.F.R. § 164.514(f) as of the Compliance Date.

2.16 mitigate, to the extent practicable, any harmful effect that is known to Provider of a use or disclosure of PHI by Provider that is not permitted by the requirements of this Appendix.

2.17 comply with all applicable federal, state and local laws and regulations.

2.18 not use, transfer, transmit or otherwise send or make available, any PHI outside of the geographic confines of the United States of America without United's advance written consent.

2.19 Government Program Requirements. To the extent that Provider receives, uses or discloses PHI pertaining to individuals enrolled in managed care plans through which United or one or more of its affiliates participate in government funded health care programs, receipt, use and disclosure of the PHI pertaining to those individuals shall comply with the applicable program requirements.

2.20 Privacy and Safeguards for NPI. Provider understands and acknowledges that to the extent it is a nonaffiliated third party under GLBA that creates or receives NPI from or on behalf of United or an Affiliate, Provider and its authorized representatives: (i) shall not use or disclose NPI for any purpose other than to perform its obligations under the Agreement; (ii) shall implement appropriate administrative, technical, and physical safeguards designed to ensure the security and confidentiality of the NPI, protect against any anticipated threats or hazards to the security or integrity of the NPI and protect against unauthorized access to or use of the NPI that could result in substantial harm or inconvenience to any consumer; and (iii) shall, for as long as Provider has NPI, provide and maintain appropriate safeguards for the NPI in compliance with this Appendix and the GLBA.

3. OTHER PERMITTED USES AND DISCLOSURES OF PHI. Unless otherwise limited in this Appendix, in addition to any other uses and/or disclosures permitted or required by this Appendix, Provider may use and disclose PHI, if necessary, for proper management and administration of Provider or to carry out the legal responsibilities of Provider, provided that the disclosures are Required by Law or any third party to which Provider discloses PHI for those purposes provides written assurances in advance that: (i) the information will be held confidentially and used or further disclosed only for the purpose for which it was disclosed to the third party or as Required by Law; and (ii) the third party promptly will notify Provider of any instances of which it becomes aware in which the confidentiality of the information has been breached.

4. TERMINATION AND COOPERATION

4.1 Termination. If United knows of a pattern or practice of Provider that constitutes a material breach or violation of this Appendix then United may provide written notice of the breach or violation to Provider and Provider must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. If Provider fails to cure the breach or end the violation within the specified timeframe, United may terminate this Appendix and the Agreement. United also may terminate this Appendix and the Agreement to the extent that any of United's applicable Covered Entity customers terminates its agreement with United.

4.2 Effect of Termination or Expiration. Within thirty (30) days after the expiration or termination for any reason (or to any extent) of the Agreement and/or this Appendix, Provider shall return or destroy all applicable PHI, if feasible to do so, including all applicable PHI in possession of Provider's subcontractors. To the extent return or destruction of the PHI is not feasible, Provider shall notify United in writing of the reasons return or destruction is not feasible and, if United agrees, may retain the PHI subject to this Section 4.2. Under any circumstances, Provider shall extend any and all protections, limitations and restrictions contained in this Appendix to Provider's use and/or disclosure of any applicable PHI retained after the expiration or termination (to any extent) of the Agreement and/or this Appendix, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.

4.3 Cooperation. Each party shall cooperate in good faith in all respects with the other party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

5. MISCELLANEOUS

5.1 Construction of Terms. The terms of this Appendix to the extent they are unclear, shall be construed to allow for compliance by the applicable Covered Entity and United with HIPAA.

5.2 Survival. Sections 4.2, 4.3, 5.1, 5.2, and 5.3 shall survive the expiration or termination for any reason of the Agreement and/or of this Appendix.

5.3 No Third Party Beneficiaries. Nothing in this Appendix shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.]

[SECURITY APPENDIX

This Appendix applies (i) when Provider requires electronic access to United Information and/or United Information Systems; (ii) in addition to any of Provider's obligations under the Agreement, any Business Associate Agreement or other agreement, or any requirements imposed upon Provider by applicable laws or regulations; and (iii) in addition to any United due diligence that may be performed regarding Provider's systems and security practices. In the event of a conflict between this Appendix and any other term between the parties, the terms most protective of United, in United's determination, shall apply.

1. Definitions. The following terms shall have the meanings as set forth below:

1.1 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of United Information or interference with the operations of any of the Provider Processing Resources. Security Incidents are classified as follows:

a) "High Severity" or severity 1 (severe impact) means external loss or exposure of United Information, causing significant impact to mission critical information technology systems including large-scale outages. Incidents or exposures classified at this level affect critical United Information Systems and will affect United's customers.

b) "Medium Severity" or severity 2 (major impact) means internal loss or exposure of United Information, causing significant business interruption. Incidents or exposures classified at this level affect non-critical United Information Systems and may affect United's customers.

c) "Low Severity" or severity 3 (moderate impact) means loss or exposure of United public information, causing a limited or confined business interruption. Incidents or exposures classified at this level affect United Information Systems or assets, but do not affect United's customers.

1.2 "United Information" includes Private and Confidential Information of United as such is defined in the Agreement, Nonpublic Personal Information, as defined under the Gramm-Leach-Bliley Act and implementing regulations ("GLB"), as well as Protected Health Information and Electronic Protected Health Information, as such terms are defined in 45 C.F.R. Parts 160 and 164 (or successor regulations).

1.3 "United Information Systems" means information systems resources supplied or operated by United or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity which are owned, controlled or administered by or on behalf of United.

1.4 "Provider Processing" means any information collection, storage or processing performed by Provider or its contractors (i) which directly or indirectly supports the services or functions now or hereafter furnished to United under the Agreement, (ii) using any United Information, or (iii) in respect of any other information if performed on behalf of United or in support of United's business, operations or services.

1.5 "Provider Processing Resources" means information processing resources supplied or operated by Provider, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Provider Processing.

2. Security Management

2.1 Provider Security Contact. Provider shall provide a security representative as the single point of contact for United on all security issues, who shall be responsible for overseeing compliance with this Appendix.

2.2 Policies and Procedures. Provider shall maintain written security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, availability, or security of Provider Processing Resources and/or United Information. Such policies and procedures shall (i) assign specific data security responsibilities and accountabilities to specific individual(s); (ii) include a formal risk management program which includes periodic risk assessments; and (iii) provide an adequate framework of controls that safeguard United Information Systems and United Information.

2.3 Infrastructure Protection. Provider shall maintain industry standard procedures to protect Provider Processing Resources, including, at a minimum:

(a) Formal security programs (policies, standards, processes, etc.);

(b) Processes for becoming aware of, and maintaining, security patches and fixes;

(c) Router filters, firewalls, and other mechanisms to restrict access to the Provider Processing Resources, including without limitation, all local site networks which may be accessed via the Internet (whether or not such sites transmit information);

(d) Resources used for mobile access to United Information Systems shall be protected against attack and penetration through the use of firewalls; and

(e) Processes to prevent, detect, and eradicate malicious code (e.g., viruses, etc.) and to notify United of instances of malicious code detected on Provider Processing Resources or affecting United Information.

3. Risk Management

3.1 General Requirements. Provider shall maintain appropriate safeguards and controls and exercise due diligence to protect United Information and Provider Processing Resources against unauthorized access, use, and/or disclosure, considering all of the below factors. In the event of any conflict or inconsistency, Provider shall protect the United Information and Provider Processing Resources in accordance with the highest applicable requirement:

(a) Federal, state, legal and regulatory requirements;

(b) Information technology and healthcare industry best practices;

(c) Sensitivity of the data;

(d) Relative level and severity of risk of harm should the integrity, confidentiality, availability or security of the data be compromised, as determined by Provider as part of an overall risk management program;

(e) United's data security requirements, as set forth in this Appendix, the due diligence process and/or in the Agreement; and

(f) Any further information security requirements which are included in a statement of work or equivalent document which is attached to or relates to the Agreement.

3.2 Security Evaluations. Provider shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with

respect to the confidentiality, integrity, availability, and security of United Information and Provider Processing Resources. Provider shall document the results of these evaluations and any remediation activities taken in response to such evaluations, and provide to United a copy.

3.3 Internal Records. Provider shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Provider shall take appropriate action to address and remediate identified vulnerabilities to United Information and Provider Processing Resources.

3.4 United Audits. Provider agrees to permit United, its auditors, its customers, or any governmental authority, upon reasonable advance notice, to inspect and examine Provider Processing Resources, the facilities used to perform Provider Processing, as well as policies, procedures, plans, and other records and documentation as reasonably necessary for United to verify Provider's compliance with this Appendix. United reserves the right to require Provider to install appropriate systems management and security software to ensure appropriate protection is in place. United shall not disclose any information learned by United in the course of performing any such inspection or examination except as may be reasonably necessary for United to comply with obligations relating to the protection of United Information or as may otherwise be required by law.

3.5 Remediation. Provider will remedy any High Severity security exposure or finding discovered by United within twenty-four (24) hours from the time the finding is identified and notice is provided to Provider. Provider will remedy any Medium to Low Severity security exposure or finding discovered by United within two (2) to five (5) business days, from the time the finding is identified and notice is provided to Provider. If Provider does not address the exposure or finding within the applicable time obligation, United shall have the right to immediately terminate access to United Information Systems and United Information without penalty to the services related to the access.

3.6 Audit Practices. Provider shall provide to United, at least annually, information on its audit processes, procedures and controls, including a report on any findings and remediation efforts. Provider shall also provide to United an independent attestation of Provider's security practices and process controls that provide sufficient evidence of such practices and controls (e.g., Statements on Auditing Standards 70 Type II equivalent, etc.).

3.7 Provider Locations. Unless previously authorized by United in writing, all work performed by Provider related to the Agreement shall be performed from the Provider location(s) designated in the Agreement and/or relevant Statement of Work(s). For any location(s) outside of the 50 United States ("Offshore Locations"), where Provider performs work related to the Agreement for United, Provider also agrees to maintain the following security controls:

(a) Provider shall conduct either a SAS70 Type II Audit, a BS-7799 certification, or an ISO27001 certification at all Offshore Locations from which work is performed by Provider related to the Agreement and will provide the resulting audit reports to United. The audits or certifications will be conducted once annually, and each report will cover a twelve month term. The audit report will be issued to United no later than 30 days after the audit is completed.

(b) Provider shall conduct assessments of general control objectives, as defined by United. These objectives may be periodically updated by United, effective upon delivery to Provider to address additional Services that Provider will provide to United.

(c) Provider will comply with all future BS-7799 regulations, ISO27001 standards, or that of its successor(s), as issued by the SEC and the Public Company Accounting Oversight Board, British Standards Institute (BSI), or International Standards Organization (ISO).

(d) In the event that Provider's audit report does not meet United requirements, United may exercise its rights under Section 3.4 of this Appendix. All costs associated with such audit(s) shall be paid by Provider.

(e) At United's request, Provider will provide a quarterly management representation letter reflecting any material changes in the environment utilized for the provided Services.

4. Personnel Security

4.1 Access to United Information. Provider shall require its employees, contractors and agents who have, or may be expected to have, access to United Information or United Information Systems to comply with the provisions of the Agreement, including this Appendix and any confidentiality agreement(s) or Business Associate Agreement(s) binding upon Provider. Provider will remain responsible for any breach of this Appendix by its employees, contractors, and agents.

4.2 Security Awareness. Provider shall ensure that its employees and contractors remain aware of industry standard security practices, and their responsibilities for protecting the United Information. This shall include, but not be limited to:

(a) Protection against malicious software (such as viruses);

(b) Appropriate password protection and password management practices; and

(c) Appropriate use of workstations and computer system accounts.

4.3 Sanction Policy. Provider shall maintain a sanction policy to address violations of Provider's internal security requirements or security requirements which are imposed on Provider by law, regulation, or contract.

4.4 Supervision of Workforce. Provider shall maintain processes for authorizing and supervising its employees, temporary employees, and independent contractors and for monitoring access to United Information, United Information Systems and/or Provider Processing Resources.

4.5 Background Checks. Provider shall maintain processes to determine whether a prospective member of Provider's workforce is sufficiently trustworthy to work in an environment which contains Provider Processing Resources and United Information. At a minimum, such processes shall meet the requirements set forth in the Background Investigations Appendix to the Agreement.

5. Physical Security. Provider shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Provider Processing Resources and areas in which United Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). Provider shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained. Provider shall maintain appropriate records of maintenance performed on Provider Processing Resources and on the physical control mechanisms used to secure Provider Processing Resources. Provider shall obtain United's prior written approval prior to moving storage or processing of United Information, or personnel which have access to United Information or United Information Systems, to a location outside the U.S.

6. Software

6.1 Software Licensing. Any access provided to Provider under this Appendix is limited to United Information and United Information Systems and United is not granting Provider a license to use the software programs contained within United Information Systems. Any license to the software programs

contained within the United Information Systems shall be pursuant to a separate agreement between the parties.

6.2 Software Usage. Provider shall not attempt to reverse engineer or otherwise obtain copies of the software programs contained in United Information Systems. This Appendix does not transfer Provider title of any ownership rights or rights in patents, copyrights, trademarks and trade secrets included in United Information Systems.

7. Security Monitoring and Response

7.1 Incident Response. Provider shall maintain formal processes to detect, identify, report, respond to, and resolve Security Incidents in a timely manner.

7.2 Incident Notification. Provider shall notify United in writing and provide a resolution plan within two (2) hours of any Security Incident(s) which result in, or which Provider reasonably believes may result in, unauthorized access to, modification of, or disclosure of United Information, United Information Systems or other United applications.

7.3 Incident Resolution. After obtaining a written notification and resolution plan, United will determine the severity of the Security Incident and advise Provider of such severity. If United considers the risk to be a High Severity exposure, Provider must resolve or mitigate the High Severity within twenty-four (24) hours of providing such notice. If United considers the exposure a Medium or Low Severity exposure, then Provider must resolve or mitigate the risk within two (2) to five (5) business days of providing such notice. If Provider does not resolve the Security Incident within the applicable time obligation, United shall have the right to immediately terminate access to United information and United Information Systems without penalty.

7.4 Site Outage. Provider shall promptly report to United any Provider site outages where such outage may impact United or Provider's ability to fulfill its obligations to United.

8. Communication Security

8.1 Exchange of Confidential Information. The parties agree to utilize a secure method of transmission when exchanging Confidential Information electronically.

8.2 Encryption. Provider shall maintain encryption, in accordance with standards mutually agreed upon between the parties, for all transmission of United Information via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

(a) Sessions between web browsers and web servers;

(b) Email containing United Information (including passwords); and

(c) Transfer of files via the Internet (e.g., FTP).

8.3 Protection of Storage Media. Provider shall ensure that storage media containing United Information is properly sanitized of all United Information or is destroyed prior to disposal or re-use for non-Provider Processing. All media on which United Information is stored shall be protected against unauthorized access or modification. Provider shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Provider Processing or on which United Information has been stored.

8.4 Data Integrity. Provider shall maintain processes to prevent unauthorized or inappropriate modification of United Information, for both data in transit and data at rest.

9. Access Control

9.1 Identification and Authentication. All access to any United Information or any Provider Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes which establish the identity of the person or entity requesting access to United Information and/or Provider Processing Resources. "Authentication" refers to processes which validate the purported identity of the requestor. For access to United Information or Provider Processing Resources, Provider shall require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique approved by United in writing. Provider shall obtain written approval from United prior to using digital certificates as part of Provider's Identification or Authorization processes. Provider shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Provider and/or used by Provider in connection with the Agreement.

9.2 Account Administration. Provider shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Provider Processing Resources and United Information. These processes shall be required for both United-related accounts and Provider's internal accounts for Provider Processing Resources, and shall include procedures for granting and revoking emergency access to Provider Processing Resources and United Information. All access by Provider's employees or contractors to United Information Systems shall be subject to advance approval by United and shall follow United standard policies and procedures.

9.3 Access Control. Provider shall maintain appropriate access control mechanisms to prevent all access to United Information and/or Provider Processing Resources, except by (i) specified users expressly authorized by United and (ii) Provider personnel who have a "need to access" to perform a particular function in support of Provider Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Provider shall maintain processes to ensure that employee or contractor access to Electronic Protected Health Information is revoked no later than 2 business days upon termination. Provider shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access United Information or Provider Processing Resources.

10. Network Security

10.1 Authorized Access. Provider shall only have access to United Information Systems authorized by United and shall use such access solely for providing services to United. Provider shall not attempt to access any applications, systems or data which United has not authorized Provider to access or which Provider does not need to access in order to perform services for United. Provider further agrees to access such applications, data and systems solely to the extent minimally necessary to provide services to United. Provider's attempt to access any applications, data or systems in violation of the terms in this Section 10.1 shall be a material breach of the Agreement.

10.2 Remote Access Requirements. In the event United authorizes Provider to remotely access United Information Systems, Provider shall only do so only from locations approved by United in writing. These locations may include, but are not limited to, Provider primary locations, co-locations, employee home offices, and required business travel destinations. Provider remote access shall be subject to United security and audit controls as referenced below in sections 10.3 and 10.4.

10.3 Remote Access Security Controls. In the event United authorizes Provider to remotely access United Information Systems, unless authorized by United in writing, only United-owned and maintained mobile/PC devices (i.e., laptops, electronic notebooks, desktop PCs, etc.) may be used for remote access

into United Information Systems. In the event that United approves Provider-owned mobile/PC devices for remote access connections, Provider agrees to the following security controls:

(a) Provider shall procure mobile/PC devices and related operational hardware, manage the facilities used for remote or at-home use, and provision access to United systems.

(b) Provider shall establish mutually agreed upon policies, procedures and protocols that are to address the facilities requirements for remote or at home access.

(c) Mobile/PC devices shall be registered with the United security guard or the United manager, as required.

(d) Provider shall restrict administrative rights to mobile/PC device and will provide United field support the rights necessary to verify configuration on periodic basis.

(e) Provider shall configure the mobile/PC device according to United's connectivity requirements, including approved VPN software.

(f) Provider will maintain mobile/PC device password and screen saver safeguards.

(g) Provider shall disable all wireless capability from the mobile/PC device when not in use.

(h) Provider shall only use current, commercially supported operating systems on the mobile/PC device.

(i) Provider shall only use current and up to date patches, hot fixes, and service. United reserves the right to require installation of appropriate systems management and security software to ensure adequate protection.

(j) Provider shall not simultaneously connect to the United network and a non-secure network (third party network or other non-standard connections).

(k) Provider may only connect to United Information Systems through a United approved network.

(l) Provider remote access users shall adhere to United standard authentication protocols including, but not limited to, network and application login accounts, and/or two factor authentication tokens.

(m) Provider shall remotely connect to United systems using only the following United-provided solutions:

(i) External Corporate Connection through a dedicated private network connection and/or via Virtual Private Network Business To Business Internet Connection ("VPN B2B"), with appropriate firewall rules to restrict connectivity to only required resources, or

(ii) External Corporate Connection Virtual Private Network Client solution to a specified user group to restrict connectivity to only required resources, or

(iii) External Corporate Connection with a CITRIX presentation model, restricting connectivity and access to only required resources.

10.4 Remote Access Audit Controls. Unless authorized by United in writing, all contracted work by Provider shall be conducted from the designated Provider locations as referenced in the Agreement and/or relevant Statement of Work(s). If United authorizes Provider personnel to provide services to United remotely (from a site not identified in the designated Provider list), the following audit controls shall apply:

(a) Provider shall monitor remote or at home users on a periodic basis, which shall include both quarterly onsite audits and a summary report on findings and remediation efforts. Provider shall provide such reports to United.

(b) Provider shall follow the additional confidentiality obligations:

(i) Provider will not remove any United Information from Provider location(s), and will not print or download any including information resulting from connectivity or access to a United system(s), without prior approval of United.

(ii) Provider shall inventory any United Information obtained by Provider and shall return or destroy United Information as required by United. If requested by United, Provider shall provide a certificate of secure destruction.

(iii) Provider will comply with all United policies and procedures regarding the safekeeping of United Information. Policies and procedures must include limitations regarding the storage of information on mobile/PC devices.

(iv) Provider will keep any United Information, in a locked file cabinet, when such information is not in use.

(v) Provider will maintain written security management policies and procedures regarding secure possession of United Information when traveling and utilizing United Information in public environments.

11. Software Development. If the Agreement involves the development of software product(s) for United, such software shall be developed and maintained in accordance with the development methodology specified by United. Such software shall satisfy the appropriate United information security policies and guidelines that are furnished by United to Provider (which are incorporated herein by reference). Provider shall comply with any instructions, guidelines or minimum compliance controls that are furnished by United to Provider (which are incorporated herein by reference) to enable United to comply with the Sarbanes Oxley Act and/or other applicable laws and regulations.

12. Business Continuity Management. Provider will, at its sole expense, establish and maintain (i) written business continuity plans for the Services and supporting facilities and (ii) written disaster recovery plans for critical technology and systems infrastructure and (iii) proper risk controls (collectively, the "Contingency Plans") to enable continued performance under this Agreement in the event of a disaster or other unexpected break in Services. Provider will update and test the operability of any applicable Contingency Plan at least annually, and will maintain each such plan upon the occurrence of a disaster event. As used herein, a disaster is defined as an unanticipated incident or event, including, without limitation, force majeure events, technological accidents, or human-caused events, that may causes a material service or critical application to be unavailable without any reasonable prediction for resumption, or that causes data loss, property damage or other business interruption without any reasonable prediction for recovery, within a commercially reasonable time period.

13. Compliance with Laws. Provider shall comply with all federal, state and local laws, regulations, ordinances and requirements relating to the confidentiality, integrity, availability, or security of United Information applicable to Provider's obligations under the Agreement. In relation to and in conjunction with Provider's obligations under any Business Associate Agreement, Provider shall maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of United as required by 45 CFR, Part 164, Subpart C.

14. Third Parties. Provider shall ensure that any agent, including a subcontractor, to whom Provider provides Electronic Protected Health Information agrees to maintain reasonable and appropriate safeguards to protect such Electronic Protected Health Information; provided, however, that Provider shall not assign, delegate, or subcontract any obligation of Provider owed to United in violation of the Agreement.

15. Amendments. This Appendix may be modified by a written agreement executed by Provider and United. Notwithstanding the foregoing or anything else, United may amend this Appendix by providing thirty (30) days advance written notice of such amendment if United reasonably determines that such amendment is necessary for United to comply with the Standards for Privacy of Individually Identifiable Health Information or the Security Standards for the Protection of Electronic Protected Health Information (both of which are set forth at 45 CFR Parts 160 and 164) or any other federal, state or local law, regulation, ordinance, or requirement relating to the confidentiality, integrity, availability, or security of individually identifiable medical or personal information.]