

**JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS**

AGENDA REQUEST

TO: Board of County Commissioners
Philip Morley, County Administrator

FROM: Erin Lundgren, Clerk of the Board

DATE: January 6, 2014

SUBJECT: **AGREEMENT re: Compliance with the Health Insurance Portability and Accountability Act (HIPAA) as Amended to Assure Certain Protections for the Privacy and Security of Protected Health Information and Prohibit the Disclosure or Use of Protected Health Information; First Choice Health Network, Inc.**

STATEMENT OF ISSUE:

The Department of Health and Human Services has established regulations implementing the privacy requirements and security requirements set forth in the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009. The privacy rule and security rule: 1) require the County update the agreement with the provider of the Employee Assistance Program, First Choice Health Network, Inc. in order to assure certain protections for the privacy and security of protected health information; and 2) prohibit the disclosure or use of protected health information to or by either party if such a contract is not in place.

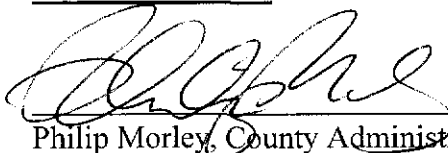
FISCAL IMPACT:

None.

RECOMMENDATION:

Approve and sign the agreement.

REVIEWED BY:


Philip Morley, County Administrator

01/02/14
Date

Business Associate Agreement

This Business Associate Agreement ("Agreement") is made and entered into by and between Jefferson County, ("Company"), and First Choice Health Network, Inc. Company and First Choice Health Network, Inc. may be referred to individually as a "Party" and collectively as the "Parties".

Recitals

WHEREAS, the Parties are considered Business Associates as such term is defined in 45 C.F.R. § 160.103.

WHEREAS, The Parties have entered into an agreement pursuant to which the Parties will provide certain services to or on behalf of each other, and each Party may create, receive, maintain, transmit, or have access to Protected Health Information in order to provide those services ("Services Agreement");

WHEREAS, the Department of Health and Human Services ("HHS") has promulgated regulations at 45 Code of Federal Regulations ("C.F.R.") Parts 160 and 164 implementing the privacy requirements ("Privacy Rule") and regulations at 45 C.F.R. Parts 160, 162 and 164 implementing the security requirements ("Security Rule") set forth in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") as amended by regulations implementing Subtitle D of the Health Information Technology for Economic and Clinical Health Act which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5);

WHEREAS, the Privacy Rule and Security Rule require Parties to enter into a written contract in order to assure certain protections for the privacy and security of Protected Health Information, and the Privacy Rule and Security Rule prohibit the disclosure or use of Protected Health Information to or by either Party if such a contract is not in place;

WHEREAS, both Parties mutually agree to satisfy the foregoing regulatory requirements and all federal, state and local confidentiality, privacy, and security laws through this Agreement;

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions.

Terms used, but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 C.F.R. Part 160, Part 162, and Part 164, then in effect or as amended, which are collectively referred to as the "HIPAA Rules".

- 1.1 **"Breach"** shall have the same meaning as the term "Breach" in 45 C.F.R. § 164.402.
- 1.2 **"Covered Entity"** shall have the same meaning given such term in 45 C.F.R. § 160.103.
- 1.3 **"Data Aggregation"** shall have the meaning given such term in 45 C.F.R. § 164.501.
- 1.4 **"Designated Record Set"** shall have the meaning given to such term in 45 C.F.R. § 164.501.
- 1.5 **"Disclose"** and **"Disclosure"** mean, with respect to Protected Health Information, the release, transfer, provision of, access to, or divulging in any other manner of Protected Health Information outside a Party's internal operations or to persons or entities other than members of its workforce.
- 1.6 **"Electronic Protected Health Information" or "EPHI"** shall have the meaning found in the Security Rule, 45 C.F.R. § 160.103.

- 1.7 **"HITECH Act"** shall mean the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005, and the regulations promulgated thereunder by the Secretary.
- 1.8 **"Individual"** shall have the same meaning found in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- 1.9 **"Protected Health Information" or "PHI"** shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created, received, maintained, or transmitted by one Party from or on behalf of the other Party pursuant to this Agreement.
- 1.10 **"Required by Law"** shall have the same meaning found in 45 C.F.R. § 164.103.
- 1.11 **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- 1.12 **"Unsecured PHI"** shall have the same meaning as the term "unsecured protected health information" in 45 C.F.R. § 164.402.
- 1.13 **"Use" or "Uses"** shall mean, with respect to Protected Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within a Party's internal operations.

2. **Authorized Uses and Disclosures.**

2.1 *General Use and Disclosure*

Except as otherwise limited in this Agreement, a Party may Use or Disclose PHI on behalf of the other Party as necessary to provide services as set forth in the Services Agreement, if such Use or Disclosure of PHI would not violate the Privacy Rule if done by a Covered Entity.

2.2 *Business Activities*

2.2.1 Unless otherwise limited herein, the Parties may Use PHI:

- (a) As necessary for their proper management and administration or to carry out their legal responsibilities;
- (b) To provide Data Aggregation services as permitted by 42 CFR § 164.504(e)(2)(i)(B);
- (c) To De-identify any and all PHI created, received, maintained, or transmitted by one Party on behalf of the other Party, provided that the De-identification conforms to the requirements of the HIPAA Rules. Such resulting De-identified information is not PHI and is not subject to the terms of this Agreement; and
- (d) As Required by Law.

2.2.2 Unless otherwise limited herein, the Parties may Disclose PHI for their proper management and administration, or to carry out their legal responsibilities provided that:

- (a) The Disclosure is Required by Law; or
- (b) the Disclosing Party obtains reasonable assurances from the person to whom the PHI is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the person, and the

person notifies the Disclosing Party of any instances of which it is aware in which the confidentiality of the PHI has been breached.

3. Business Associate Obligations.

3.1 Use of PHI

The Parties shall not Use or further Disclose PHI other than as permitted or required by the Services Agreement, this Agreement, or as Required by Law. In Using, Disclosing, or requesting PHI from one Party, the other Party agrees to limit PHI to the minimum necessary to accomplish the intended purpose of such Use, Disclosure, or request. "Minimum necessary" shall be interpreted in accordance with the HITECH Act and the HIPAA Rules, and implementing regulation or guidance on the definition.

3.2 Appropriate Safeguards; Compliance with Security Rule

The Parties shall use appropriate administrative, technical, and physical safeguards to prevent Use or Disclosure of PHI other than as provided for by this Agreement. Each Party shall comply with the Security Rule and shall implement administrative, physical, and technical safeguards (including written policies and procedures) that will reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI it creates, receives, maintains, or transmits on behalf of the other Party.

3.3 Disclosure to Subcontractors

Each Party agrees to ensure that any subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees to comply with the applicable HIPAA Rules and the same restrictions and conditions that apply through this Agreement with respect to such PHI by entering into a Business Associate Agreement with the subcontractor consistent with 45 C.F.R. 164.502(e).

3.4 Delegation of Covered Entity's Duties

To the extent either Party is to carry out one or more of a Covered Entity's obligations under the Privacy Rule, such Party shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

3.5 Disclosure Accounting

Each Party agrees to document all Disclosures of PHI and information related to such Disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of Disclosures in accordance with 45 C.F.R. § 164.528 ("Disclosure Information") and to retain such documentation for six (6) years from the date of Disclosure.

Within thirty (30) calendar days after receipt of a written notice from one Party of a request by an Individual or Covered Entity for an accounting of Disclosures of PHI, the other Party shall provide to the requesting Party the Disclosure Information necessary to enable a Covered Entity to meet the Disclosure accounting obligations under 45 C.F.R. § 164.528. In the event a request for an accounting regarding PHI of one Party is delivered directly to the other Party or its subcontractors, the Party who received the request shall within ten (10) calendar days after receipt forward such request to the other Party, to enable that other Party to deliver the request to the Covered Entity to whom the disclosure accounting obligation under 45 C.F.R. § 164.528 applies. Within twenty (20) calendar days after forwarding the request to the other Party, the Party who initially received the request shall provide its Disclosure Information to the other Party. It shall be the requesting Party's responsibility to prepare and deliver any accounting of disclosures to the Covered Entity. Both Parties (who are Business Associates) will include, in any Disclosure Information, the information listed in 45 C.F.R. § 164.528(b).

3.6 *Access to PHI*

Within fifteen (15) calendar days following one Party's request, the other Party shall make available to the requesting Party or, at the written direction of the requesting Party, to an Individual, for inspection and copying PHI about the Individual that is in a Designated Record Set maintained by the Party to whom such request is made, so that the requesting Party may deliver such information to the Covered Entity, who must meet its access obligations under 45 C.F.R. §164.524. If either Party requests an electronic copy of PHI that is maintained by the other Party electronically in a Designated Record Set, the Party to whom the request is made will provide an electronic copy in the form and format specified by the requesting Party in accordance with 45 C.F.R. § 164.524(c)(2). Any denial of access by an Individual to the PHI requested shall be the responsibility of the Covered Entity to whom the access obligation under 45 C.F.R. §164.524 applies.

3.7 *Amendment of PHI*

Upon receipt of a request from one Party, the other Party shall promptly amend or make available to the requesting Party for amendment, an Individual's PHI it maintains in a Designated Record Set to enable the requesting Party to make such information available to the Covered Entity who must meet its obligations under 45 C.F.R. § 164.526. Any denial of a request by an Individual for amendment of PHI maintained pursuant to the Agreement shall be the responsibility of such Covered Entity.

3.8 *Government Access to Books and Records*

Each Party shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received on behalf of the other Party, available to the Secretary for purposes of determining the Parties' compliance with the HIPAA Rules. In such case, unless prohibited by law or court or order, each Party shall provide to the other Party, (i) prompt written notice of its receipt of any such request from the Secretary, and (ii) a copy of any documentation, books, and records provided to the Secretary pursuant to the Secretary's request.

3.9 *Reporting and Mitigation of Unauthorized Use and Disclosure of PHI or Breach of Unsecured PHI*

3.9.1 Reporting of Unauthorized Use and Disclosure of PHI. Each Party shall provide a written report to the other Party of any Uses or Disclosures of PHI not authorized by the Services Agreement or this Agreement of which it becomes aware not more than thirty (30) calendar days after the unauthorized Use or Disclosure is discovered.

3.9.2 Reporting of Breach of Unsecured PHI. Each Party shall notify the other Party within thirty (30) calendar days following the discovery of a suspected or actual Breach of Unsecured PHI. A suspected or actual Breach shall be treated as discovered as of the first day on which the Breach is known, or, by exercising reasonable diligence would have been known, to the Party that caused the Breach. If a delay is requested by a law enforcement official in accordance with 45 C.F.R. § 164.412, the Parties may delay notification for the applicable period of time.

3.9.3 Content of Notice. The notice of unauthorized Use or Disclosure, or of Breach of Unsecured PHI, shall include:

(a) To the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been improperly accessed, acquired, Used or Disclosed;

(b) Information related to the unauthorized person or persons who impermissibly Used the PHI or to whom the improper Disclosure was made, and whether the PHI was actually acquired or viewed;

(c) The nature of the Breach or other non-permitted Use or Disclosure, including a brief description of what happened, the date of the non-permitted Use or Disclosure or Breach and the date of discovery;

(d) A description of the types of Unsecured PHI that were involved in the non-permitted Use or Disclosure or Breach, including the nature of services, types of identifiers, and the likelihood of re-identification, including whether full name, social security number, credit card number, date of birth, home address, account number, diagnosis, medication, treatment plan, or other information were involved;

(e) The corrective or investigative action taken or that will be taken to prevent further non-permitted Uses or Disclosures, to protect against future Breaches, and the extent to which the risk to the PHI has been mitigated;

(f) Any details necessary for the non-Breaching Party to conduct a risk assessment to determine the probability that the PHI believed to have been improperly accessed, acquired, Used or Disclosed has been compromised and the steps the affected Individuals should take to protect themselves; and

(g) Such other information, including a written report, as the non-Breaching Party may reasonably request.

3.9.4 **Costs of Breach Notification and Mitigation.** Each Party shall, at its own cost and expense, mitigate to the extent practicable, any harmful effects known to it of any Use or Disclosure of PHI in violation of the requirements of this Agreement. To the extent that the non-Breaching Party determines that the Breach notification requirements of the HIPAA Rules are triggered by a Breach of Unsecured PHI as described in Section 4.3 below, the breaching Party shall reimburse the non-breaching Party for all reasonable and necessary costs related to such notifications.

3.9.5 **Security Incidents.** Both Parties will report to each other any attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of the other Party's Electronic Protected Health Information or interference with system operations in their respective information system of which they become aware. The Parties acknowledge that probes and reconnaissance scans are commonplace in the industry and, as such, the Parties acknowledge and agree that, to the extent such probes and reconnaissance scans constitute Security Incidents, this Section 3.9.5 constitutes notice of the ongoing existence and occurrence of such Security Incidents for which no additional notice to either Party shall be required, as long as such probes and reconnaissance scans do not result in unauthorized access, Use, or Disclosure of PHI. Probes and reconnaissance scans include, without limitation, pings and other broadcast attacks on a Party's firewall, port scans, and unsuccessful log-on attempts that do not result in unauthorized access, Use or Disclosure of PHI.

3.9.6 **State Law Requirements.** In the event either Party has an independent notification obligation related to impermissible Use or Disclosure of PHI in connection with this Agreement or the Services Agreement, such Party shall promptly notify the other Party of such obligation and, at least five (5) business days before giving any such notice, shall notify the other Party of its intent to provide the required notifications, including any related information required by applicable state law.

3.10 *Retention of PHI*

Each Party shall retain all PHI throughout the term of this Agreement and shall continue to maintain such information not otherwise returned or destroyed pursuant to Section 5.4 of this Agreement for a period of six (6) years after the termination of this Agreement.

3.11 *Restrictions on Disclosures*

Each Party will comply with written notice from the other Party to provide for confidential communications of PHI, or to restrict the Use or Disclosure of PHI, pursuant to 45 C.F.R. § 164.522, including any request by an Individual to restrict the Disclosure of the Individual's PHI to a health plan if the Disclosure is (1) for the purpose of carrying out payment or health care operations, is not for purposes of carrying out treatment, and it not otherwise Required by Law, and (2) the PHI pertains solely to a health care item or service for which the Individual, or person other than the health plan on behalf of the Individual, has paid in full.

3.12 *Prohibition on Sale of PHI*

Except as otherwise expressly permitted by the HIPAA Rules, the Parties shall not directly or indirectly receive remuneration, including financial or non-financial remuneration, in exchange for an Individual's PHI unless a valid authorization that meets the requirements of 45 C.F.R. § 164.508 is obtained and states that the disclosure will result in remuneration.

3.13 *Standard Transactions.*

Each Party shall comply with the HIPAA Rules' Standards for Electronic Transactions when conducting any Standard Transactions on behalf of the other Party.

4.1 With regard to the Use and/or Disclosure of Protected Health Information, each Party agrees to:

4.1.1 *Notice of Privacy Practices*

Provide the other Party in a timely manner a written or electronic copy of the notice of privacy practices (the "Notice") that is provided to Individuals in accordance with 45 C.F.R. § 164.520, including any limitation(s) in such Notices to the extent that such limitation may affect the other Party's Use or Disclosure of PHI.

4.1.2 *Restrictions*

Notify the other Party in writing of any restrictions to the Use or Disclosure of PHI that it has agreed to in accordance with 45 C.F.R. § 164.522 to the extent that such restriction may affect the other Party's Use or Disclosure of PHI. Each Party will promptly notify the other Party in writing of the termination of any such restriction requirement and whether any of the PHI will remain subject to the terms of the restriction agreement.

4.1.3 *Authorizations*

Inform the other Party, in writing and in a timely manner, of any changes in, or revocation of an authorization provided to it by an Individual or Covered Entity to Use or Disclose PHI to the extent that such changes may affect the other Party's Use or Disclosure of PHI.

4.1.4 *Confidential Communications*

Notify the other Party in writing and in a timely manner, of any confidential communications requests related to an Individual's PHI that it has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such request may affect the other Party's Use or Disclosure of PHI. Each Party will promptly notify the other Party in writing of the termination of any such confidential communications requirement.

4.2 The Parties shall not request each other to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule if done by a Covered Entity.

4.3 *Determination of Breach and Notification Obligations*

The non-breaching Party will be solely responsible to determine whether a non-permitted Use or Disclosure constitutes a Breach and will be responsible to provide, to the extent and within the time required by the HIPAA Rules, notice to the affected Covered Entity (who in turn must provide notice to the affected Individuals, the media, and the Secretary). If the non-breaching Party determines the non-permitted Use or Disclosure is a Breach that triggers the HIPAA Rules' breach

notification requirements, then the breaching Party will reimburse the non-breaching Party for all reasonable and necessary costs related to the notifications of a Breach of Unsecured PHI created, received, maintained or transmitted by the breaching Party.

5. Term and Termination.

5.1 Term and Effective Date

This Agreement shall be effective on the effective date of the Services Agreement and shall continue in effect until all obligations of the Parties have been met, unless terminated as provided herein or by the mutual agreement of the Parties.

5.2 Termination for Material Breach

Upon one Party's determination, in its sole discretion, that the other Party has violated a material term of this Agreement, the non-violating Party will provide the violating Party with written notice of the violation and either (i) an opportunity to cure the breach or end the violation within thirty (30) calendar days after receipt of the notice or such other period determined reasonable and appropriate by the non-violating Party, or (ii) terminate this Agreement if the violating Party does not cure the breach or end the violation within such period, or (3) immediately terminate this Agreement if eliminating the violation or cure of the breach is not possible.

5.3 Termination of Agreement

This Agreement shall automatically terminate without any further action of the Parties upon the termination or expiration of the Services Agreement.

5.4 Effect of Termination

5.4.1 Upon termination of this Agreement, each Party shall return all PHI that it received from, or created or received on behalf of the other Party that it (or its subcontractors) maintained in any form. Either party may request that the other Party destroy such PHI and provide documentation evidencing such destruction, and in such case, both Parties agree to comply with such request if feasible. The Parties shall retain no copies of such PHI except as follows. If the Party to whom the request to return or destroy such PHI is made determines that return or destruction of PHI is not feasible, such Party shall provide notice to the requesting Party of the conditions that make return or destruction infeasible, and shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as it maintains such PHI.

5.4.2 In the event this Agreement is terminated for any reason, the Services Agreement will also terminate as of the effective date of termination of this Agreement.

5.5 Survival

The obligations of both Parties under this Section 5 shall survive the termination of this Agreement.

6. Miscellaneous.

6.1 *Indemnification.* Each Party shall indemnify, defend and hold harmless the other Party (including without limitation the other Party's employees, officers, directors, agents, successors and assigns) from and against any and all claims, causes of action, liabilities, damages, costs or expenses (including without limitation attorneys' fees, court costs, costs of administrative or other proceedings, and costs of investigation) arising out of or related to any breach of any of the terms and provisions of this Agreement by the indemnifying Party or any party acting by or through the indemnifying Party (including without limitation its employees, agents, representatives or Subcontractors). The obligations of the Parties under this Section 6.1 shall survive the termination of this Agreement.

- 6.2 *Compliance with Law*
Both Parties agree to comply with all federal, state, and local laws applicable to the privacy and security of health information, including but not limited to the HIPAA Rules and the HITECH Act. Upon the compliance date or other effective date of any law or final regulation or amendment to final regulation adopted by the Secretary that affects the obligations of either Party to this Agreement, this Agreement will automatically amend such that the obligations of each Party under this Agreement remain in compliance with such law or regulation. The Parties agree to take such action as is necessary to document any such amendment to this Agreement as is necessary for compliance with the requirements of the HIPAA Rules and the HITECH Act, and any other applicable law or regulation.
- 6.3 *No Third Party Beneficiaries*
Nothing in this Agreement shall confer any rights, remedies, obligations, or liabilities upon any person or other third party other than the Parties to this Agreement.
- 6.4 *Disputes*
If any controversy, dispute, or claim arises between the Parties with respect to this Agreement, the Parties shall make good faith efforts to resolve such matters informally and in accordance with the dispute resolution process specified in the Services Agreement.
- 6.5 *Interpretation*
Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits both Parties to comply with applicable HIPAA Rules and the HITECH Act. In the event of any inconsistency or conflict between this Agreement and any other agreement between the Parties, the terms and conditions of this Agreement shall have priority.
- 6.6 *Notice*
Any notice to be given hereunder shall be given in writing and in accordance with the applicable terms of the Services Agreement.
- 6.7 *Governing Law*
This Agreement shall be interpreted, enforced, and governed in accordance with the laws of the State of Washington, notwithstanding any conflict of law doctrine to the contrary.
- 6.8 *Amendments; Waiver*
This Agreement may not be modified or amended, nor shall any provision hereof be waived, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events. A failure or delay in enforcing compliance with any term or condition of this Agreement does not constitute a waiver of such term or condition unless it is expressly waived in writing.
- 6.9 *Survival*
Both Parties' obligations to protect the privacy and safeguard the security of PHI as set forth in this Agreement shall survive the termination of this Agreement.
- 6.10 *Severability*
The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.
- 6.11 *Counterparts; Electronic Copies*
This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which taken together shall constitute one and the same instrument. Electronic copies of this fully executed Agreement shall be deemed to be originals.

IN WITNESS WHEREOF, the Parties have duly executed this Agreement as of the effective date of the Services Agreement.

First Choice Health Network, Inc.

Signature: _____
Name: _____
Title: _____

Company:

Jefferson County Board of Commissioners

Signature: _____
Name: _____
Title: _____

Approved as to form only

David Alvarez 12/26/13

Jefferson Co. Prosecutor's Office
David Alvarez, Chief Civil DPA