

Highmark Inc. dba Industrial Medical Consultants (IMC)
Service Authorization Agreement ("SAA")

Client Name: Warren County School District
Client Address: 589 Hospital Drive, Suite A
Warren, PA 16365
Effective Date: September 27, 2012
Transaction #: WCSD20120927

Highmark Inc. does certain business through its division, Industrial Medical Consultants ("IMC") and is hereby authorized to provide the service(s) detailed in the Statement of Work (SOW). Services, Pricing and Scope of Work are detailed in the attached Appendix A, SOW, made a part hereof. This Authorization shall constitute an agreement between IMC and Client. Any other services not specifically detailed herein are not covered under this Authorization, and are subject to execution of a mutually acceptable authorization.

IMC and Client may each be referred to herein individually as a "Party" and collectively as the "Parties".

IMC will bill all Client claims as incurred during the month. Client agrees to make all payments in US dollars within thirty (30) days of invoice date. Late payments in excess of forty-five (45) days, will be subject to a fee of one and one-half percent (1.5%) per month from due date, excluding any billings in dispute.

Unless earlier terminated in accordance with its terms, this Authorization shall commence on the Effective Date and shall continue until December 31, 2012. Either Party may terminate this Authorization upon twenty (20) days written notice to the other Party, whether with cause or without cause and without penalty or cancellation charge. Upon termination of this Authorization, IMC agrees to return to Client any and all Client documents or other materials in its possession, except that IMC may retain a copy of those documents or materials relevant to state or federal mandated retention requirements or IMC's retention policies.

Client will provide IMC with any necessary documentation and will allow IMC adequate and timely access to Client information as necessary to meet the requirements and scope of services defined in the attached SOW or as directed by any applicable laws, orders or regulations. IMC bases its services upon its reliance upon the information provided by Client. Should this information be inaccurate or incomplete, IMC reserves the right to modify its fee structure and/or services and/or terminate this Authorization, upon reasonable prior written notice to Client.

All proprietary or confidential information disclosed by a Party (the "disclosing Party"), its subsidiaries and affiliates, to the other Party (the "receiving Party"), which is either designated as proprietary and/or confidential or by the

nature of the circumstances surrounding disclosure, ought in good faith to be treated as proprietary and/or confidential ("Confidential Information") will not be disclosed by the receiving Party to any third party and will be protected by the receiving Party from disclosure to any third party. This obligation shall survive the termination or expiration of this Authorization. Confidential Information includes, without limitation, the disclosing Party clinical protocols, manuals, modules, in service materials, documentation, forms, subscriber or covered employee data (whether or not including personally identifiable health information), provider data, medical records, financial information and reports, policies and procedures, trade secrets, business and product plans, transcription and correspondence documents, the terms of this Authorization, and other written materials provided by the disclosing Party. Upon termination of this Authorization for any reason, Client and IMC agree that neither of them will alter or otherwise use or disclose to others any Confidential Information of the other Party, which records shall be returned promptly.

Privacy Compliance. All personally identifiable information about Client's employees or members or IMC's clients ("Protected Health Information" or "PHI") is subject to various statutory privacy standards, the Health Insurance Portability and Accountability Act of 1996 and regulations adopted thereunder by the Department of Health and Human Services, 45 C.F.R. Parts 160, 162, 164 ("HIPAA"). The Parties shall treat all such information in accordance with those standards, and shall use or disclose PHI received from the other only for the purposes stated in this Authorization, or to comply with judicial process or any applicable statute or regulation.

Business Associate Provisions. The following restrictions shall apply to all uses and disclosures of all PHI.

1. In all instances where the HIPAA "minimum necessary" standard, as provided in 45 C.F.R. §164.502(b), applies, a Party shall disclose PHI to the other Party, and such Party shall collect, create or re-disclose such PHI, to the minimum extent reasonably necessary to permit the performance of such Party's duties as described in this Authorization.
2. Each Party shall use the PHI only to perform the functions delegated to it under this Authorization, and for no other purpose.
3. Each Party shall:
 - (A) Not use or further disclose PHI other than as permitted or required by this Authorization, or to comply with judicial process or any applicable statute or regulation;

(B) Notify the other Party in advance of any disclosure of PHI that said Party is required to make under any judicial or regulatory directive;

(C) Notify the other Party, and obtain the other Party's written consent, prior to engaging a subcontractor to which said Party intends to provide PHI;

(D) Store the other Party's PHI and confidential data only in secure data facilities located in the United States, and adopt security measures to assure that no person or entity physically located outside of the United States can access, acquire, use or disclose any such data;

(E) Implement reasonable and appropriate administrative, technical and physical safeguards to preserve the integrity, confidentiality and availability of PHI, and to prevent non-permitted use or disclosure of PHI. When so required:

- 1) Such safeguards shall be consistent with applicable requirements of 45 C.F.R. Part 164, Subpart C, pertaining to the security of Electronic Protected Health Information ("EPHI"), and as required by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"). Each Party also shall develop and implement policies and procedures and maintain documentation of such policies and procedures to assure compliance with the Security Rule standards as required by the HITECH Act;

- 2) Each Party shall ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect it; and

- 3) Each Party shall report any security incident (as defined in 45 C.F.R. §164.304) of which it becomes aware to the other Party.

(F) Report to the other Party any use or disclosure of PHI not provided for in this Authorization of which the Party becomes aware within five (5) business days following discovery. In addition, said Party shall report, following discovery and without unreasonable delay, but in no event later than five (5) business days following discovery, any acquisition, access, use or disclosure of "Unsecured Protected Health Information" (as defined by the HITECH Act and any implementing regulations) in a manner not permitted by the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E). Each Party shall cooperate with the other Party in investigating such unauthorized use or disclosure and in meeting the other Party's obligations under the HITECH Act and any other security breach notification laws. For purpose of this section, "discovery" shall mean the time at which the unauthorized acquisition, access,

use or discovery is known, or in the exercise of reasonable diligence should have been known, to a person (other than the person committing the breach) who is a member of the workforce of the Party, is an agent of the Party or is a member of the workforce of such agent.

Any such report shall include the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by a Party to have been, accessed, acquired or disclosed. Each Party shall make the report to the other Party's Chief Privacy Officer not more than five (5) business days after the Party learns of such non-permitted use or disclosure. The Party's report shall at least:

- 1) Identify the nature of the non-permitted access, use or disclosure, including the date of the event and the date of discovery of the event;

- 2) Identify the Protected Health Information accessed, used or disclosed (e.g., full name, social security number, date of birth, etc.);

- 3) Identify who made the non-permitted access, use or disclosure and who received the non-permitted disclosure;

- 4) Identify what corrective action the Party took or will take to prevent further non-permitted access, uses or disclosures;

- 5) Identify what the Party did or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and

- 6) Provide such other information, including a written report, as the other Party may reasonably request.

(G) Ensure that any agents, including any subcontractor approved by the other Party under subsection (C) above, to whom the Party provides PHI received from the other Party, or created or received by the Party on behalf of the other Party, agrees to the same restrictions and conditions that apply to the protection of information under this Authorization;

(H) If a Party holds any PHI in a Designated Record Set as defined by HIPAA, make PHI available to individuals as required by 45 C.F.R. §164.524, and, where applicable, the HITECH Act;

(I) If a Party holds any PHI in a Designated Record Set as defined by HIPAA, make PHI available for amendment and incorporate any amendments in accordance with 45 C.F.R. §164.526;

(J) Make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. §164.528, and, where applicable, the HITECH Act;

(K) Ensure that any of a Party's personnel, subcontractors or agents who may come into contact with the other Party's PHI undergo any privacy and security training required by the other Party prior to receiving PHI from the other Party;

(L) Complete and promptly return to the other Party any affirmation or certification requested by the other Party to monitor a Party's compliance with these provisions, which certification shall not be required more than once in any twelve (12) -month period;

(M) Upon reasonable notice, make its internal practices, facilities, books and records relating to the use and disclosure of PHI received from, or created or collected by a Party on behalf of, the other Party, available to the Secretary of Health and Human Services and/or the other Party when called upon for purposes of determining the other Party's and/or a Party's compliance with federal privacy standards; and

(N) At termination of this Authorization, if feasible, return or destroy all PHI received from the other Party, or created or received by a Party on behalf of the other Party, that Party still maintains in any form, and retain no copies of such information, or, if such return or destruction is not feasible, continue to treat all such information in accordance with the limits provided in this Authorization and limit further uses and disclosures to those purposes that make the return or destruction of the information unfeasible.

4. If the HIPAA regulations governing PHI are modified in any way affecting the Business Associate Provisions of this Authorization, as soon as reasonably possible, but no later than the compliance date for any regulation, the parties shall review this Authorization and, as necessary, modify this Authorization to incorporate any relevant provisions.

5. If the other Party determines that a Party has violated a material term of these Business Associate Provisions, the other Party is authorized, pursuant to 45 C.F.R. §164.504(e)(2)(iii), to terminate this Authorization.

6. The terms and conditions of these Business Associate Provisions shall override and control any conflicting term or condition of this Authorization. All nonconflicting terms and conditions of this Authorization remain in full force and effect.

7. If practicable and feasible, written notices to report the use or disclosure of PHI as required under this Authorization, or questions regarding the handling of PHI, shall be made by secure email to comply with timeliness requirements followed by a hard copy notice by U.S. mail or overnight delivery service. If secure email is not practicable or feasible, written notices shall be sent via facsimile followed by a hard copy notice by U.S. mail or overnight delivery service. All notices to

Client shall be sent to the Client's address below. All notices to Highmark should be addressed as follows:

Highmark Inc. Privacy Office
Fifth Avenue Place
120 Fifth Avenue
Pittsburgh, PA 15222
Telephone: 1-866-228-9424 (toll-free)
Fax: 1-412-544-4320
Email: privacy@highmark.com
Attention: Chief Privacy Officer

8. The requirements of the HITECH Act do not preempt more stringent requirements of the Centers for Medicare & Medicaid Services ("CMS") applicable to Medicare Parts A, B, C and D. In the event a Party becomes aware of a "security incident" that presents a threat to the integrity or security of CMS data on any data system said Party controls or accesses which houses CMS data, the Party is required to report to the other Party as soon as possible. For purposes of this section, the definition of "security incident" is: the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

9. Each Party agrees that all information obtained by or provided to the Party in carrying out the Services provided for hereunder, including the contents of this Authorization, shall be maintained in confidence by the Party and that the Party shall not publish nor disclose to third persons nor otherwise make use of such confidential information except for the performance of such Services hereunder. The other Party's confidential information includes, but is not limited to, the other Party's financial, account, human resources, provider and other proprietary information. This obligation shall not apply with respect to any information: (a) which is already in the possession of the Party prior to acquiring the information hereunder; (b) which is or becomes in the public domain through no fault of either party; or (c) which is rightfully obtained on a non-confidential basis from a third party.

In addition, certain categories of information, such as the other Party's employees' or members' Protected Health Information ("PHI"), is subject to protection under applicable federal and state laws and regulations. To ensure that the confidentiality of the above information is protected, each Party agrees to permit the other Party to review a Party's security practices and policies relating to the protection of such confidential information. The provisions set forth in this Paragraph shall survive any termination of this Authorization.

The services rendered under this Authorization shall be subject to that level of permissible performance established by the specific state jurisdiction under which the Employee or Claim is governed. In all events, and notwithstanding any other provision of this Authorization, each Party hereby agrees to defend, indemnify and hold harmless the other Party from and against any damages, expenses or liabilities arising out of, or related to, acts, omissions or non-performance of such Party, its subcontractors, employees and/or agents. This provision shall survive the termination or expiration of this Authorization.

All media releases and public disclosures by either IMC or Client relating to this Authorization, including promotional or marketing material, will be coordinated with and approved by the other Party prior to the release.

This Authorization, and the relevant Statements of Work constitute the complete and entire agreement and understanding between the Parties and supersedes all discussions, negotiations, agreements or understandings, whether written or oral, with respect to the subject matter hereof. No amendment or modification of this Authorization shall be valid unless made in writing and signed by the Parties.

This Authorization shall be governed by, and construed and enforced in accordance with, the laws of the Commonwealth of Pennsylvania, without regard to any choice or conflict of laws provision or rule. In the event of a dispute, Client will schedule, in a timely and expeditious manner, a meeting with IMC's designee(s) and Client representative(s) in an attempt to resolve those issues that rise to a level of breach or termination.

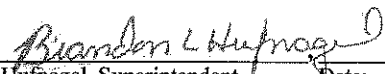
This Authorization shall not be assigned by Client, without the prior written consent of IMC.

Neither Client nor IMC shall be deemed to be in breach of this Authorization if prevented from or delayed in performing any of its obligations hereunder to the extent caused by any occurrence beyond the reasonable control of such Party, including, but not limited to, any act of God, fires, floods, natural disaster, war, terrorism, riot, civil insurrection, military hostilities, power outages, governmental or legal restrictions, labor disturbances, or intentional, reckless or negligent acts of non-related third parties, and when it relates to such time line commitments described herein not being met due to providers inability to provide necessary records and information.

IN WITNESS WHEREOF, Client and IMC have each caused this Authorization to be signed and delivered by its

duly authorized officer, all as of the date first set forth above.

Client: Warren County School District

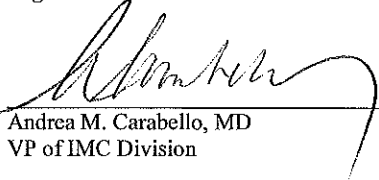

Brandon Hufnagel, Superintendant Date: 10/12/12

**Warren County School District
589 Hospital Drive, Suite A
Warren, PA 16365**

**814-723-6900 (Work)
814-688-1178 (Cell)**

hufnagelb@wcsdpa.org

Highmark Inc. dba Industrial Medical Consultants:


Andrea M. Carabello, MD Date: 10/17/12
VP of IMC Division

**120 Fifth Ave
Suite 2575
Pittsburgh, PA 15222
Phone: (412) 544-1293
Fax : (412) 235-9027**

Email: acarabello@imcdocs.com

This Authorization may be executed by facsimile and in one or more counterparts, each of which shall be deemed to be an original and all of which shall constitute one and the same agreement.