

409 North Second Street
Suite 500
Harrisburg, PA 17101-1357

Jayson R. Wolfgang
717 237 4852
Jayson.wolfgang@bipc.com

T 717 237 4800
F 717 233 0852
www.buchananingersoll.com

May 1, 2014

VIA HAND DELIVERY

Mr. Stephen J. Johnson, CPA
Deputy Insurance Commissioner
Office of Corporate and Financial Regulation
Pennsylvania Insurance Department
1345 Strawberry Square
Harrisburg, PA 17120

RECEIVED
Corporate & Financial Regulation

MAY 01 2014

**Pennsylvania
Insurance Department**

**Re: Highmark Health
Response to Conditions 7, 8 and/or 9 of the April 29, 2013 Approving
Determination and Order (Order No. ID-RC-13-06)**

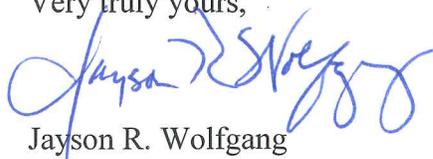
Dear Deputy Commissioner Johnson:

I am hand delivering herewith a non-confidential report in Response to Conditions 7, 8 and/or 9 of the Approving Determination and Order issued on April 29, 2013. This submission relates to the Firewall Policy.

I have provided a copy by electronic means to Mr. Beaser and Mr. Newman.

Thank you for your consideration.

Very truly yours,


Jayson R. Wolfgang

JRW/skm
Enclosure



To: Insurance Department of the Commonwealth of Pennsylvania
From: William Winkenwerder, Jr., CEO and President Highmark Health
Lisa A. Martinelli, Chief Privacy Officer Highmark Health
Date: April 29, 2014
Subject: Report of Compliance with Policy Protecting Competitively Sensitive Information

As required by Conditions 7 through 9 of the Insurance Department (Department) of the Commonwealth of Pennsylvania's Approving Determination and Order No. ID-RC-13-06 (Order), we represent that the following certifications are true to the best of our information, knowledge and belief:

Condition 7 – Policy Development and Access

Contemporaneous with Department approval, the Highmark Health Policy Protecting Competitively Sensitive Information (Approved Firewall Policy, or Policy) was effective on October 24, 2013 (Effective Date). Approved Firewall Policies for each Highmark Health Provider or Health Care Insurer (Approved Sub Policies, or Policy), as defined by the Order and as set forth in Attachment A¹ of the Policy, were effective on the same date.

7. A. Development

There have been no material amendments to, waivers, or terminations of the Approved Firewall Policy and/or Approved Sub Policies to report to Department.

Policies have been in full force and effect at all times since their respective Effective Dates, and are publicly available on their respective entity website.

Necessary and appropriate Board approvals were obtained formally adopting Policies.

Condition 8 - Compliance with Policy

At all times since the Effective Date, Highmark Health, Highmark, Inc. and its subsidiaries and affiliates that are within the scope of the Order, and the Allegheny Health Network and its subsidiaries and affiliates that are within scope of the Order (collectively "Entities), have been governed by and operated in accordance with the Policy.

The Policy has and has been fully implemented, monitored and enforced in accordance with its terms.

8. A. Implementation

Implementation of Policies occurred in a manner consistent with the requirements of the Order and the guidelines provided in Appendix 2, thereto.

8. A. (1). Prior to Effective Date of the Policy, and in anticipation of Department approval, data sharing and information management educational sessions were presented by the Chief Privacy Officer and Chief Legal Officer to executive and senior management across all applicable Entities. The information provided during these sessions described the creation and importance of logical and technical firewalls, and the establishment of processes for appropriate data sharing, and for reporting any inappropriate sharing to management, as may be necessary.

The Highmark Health Privacy Department developed a formal training module for all personnel with access to Competitively Sensitive Information (CSI), entitled "Protecting CSI: Competitively Sensitive Information." This 1-hour online module specifically addresses the terms and conditions of the Policy, the processes for compliance with it, and provides illustrative examples of appropriate and inappropriate disclosures of data. A portable CD version of the module was also produced for certain Personnel who are offsite or work remotely. Call-to-action cards were designed as a compliance reminder tool for all Personnel. The card contains the definition of CSI as well as the location of the Policy and the process for reporting violations or suspected violations. They were produced and continue to be distributed to Personnel.

From the period of November 1, 2013 through March 17, 2014, all thirty-eight thousand three-hundred sixty-one, (38,361) personnel who have access to Competitively Sensitive Information (Personnel) completed the training module. In addition, this training has been included in the onboarding orientation process for newly hired Personnel. All Personnel acknowledge and agree through either electronic or paper certification that they have completed the training, that they have read the Policy, have access to a copy of the policy, understand the Policy, and agree to abide by the Policy.²

Supplemental targeted training was provided by the Chief Privacy Officer at the request of business units and will be provided at the request of management.

Refresher training will be provided at least annually to all Personnel. All Personnel who have access to CSI are required to certify that they have completed the training, that they have, accessed, read and understand the policy, and they agree to abide by it.

Certain contractors who access CSI in the ordinary course of their work were provided with copies of the policy and asked to sign attestations through various online vendor management tools.

Training was provided to members and directors of all Boards that are expected to comply with the Policy and will receive refresher training at least annually. The Audit Committees of the Boards are periodically apprised of the monitoring and policy compliance.

8. A. (2) Subsequent to the Effective Date of the Policy, a process was established at Highmark Health to discuss, review, analyze and memorialize requests for data sharing between Entities for specific approved purposes. This process was created to help ensure that data compiled for appropriate business purposes does not inadvertently or unintentionally violate Policy. The process also provides formal opportunities for Personnel who are uncertain if a particular use of data might potentially violate Policies to bring their question to a subject matter expert for review and analysis.

To ensure that proposed data sharing does not implicate or violate Policies, Personnel are expected to submit questions concerning requests for data sharing, including the business justification for the data, to Infomgmtdecisions@highmarkhealth.org. The Chief Privacy Officer receives all requests directly. These requests are submitted to the CSI Firewall Committee which meets bi-weekly to review, approve or deny requests to share data. All data requests and final determinations are recorded and tracked by a designated Committee member and retained with supporting documentation in a database accessible only to Committee members.

8. A. (3) The Highmark Health Chief Privacy Officer, Director of Privacy or Senior Privacy Official (PO) for each Entity conducted a good faith review and certified compliance with its Policy since the Effective Date. This review and certification further represents that CSI was not used for any inappropriate purpose including disadvantaging rival competitor Health Care Provider or Health Care Insurer. In addition to this Report of Compliance, a signed attestation of compliance from each PO is on file with the Highmark Health Privacy Department.

8. B. Monitoring and Auditing

Commencing with the Effective Date, processes for monitoring Policy compliance were developed and implemented. These processes were developed under the direction of the Chief Privacy Officer, Chief Information Security Officer and Chief Auditor and Compliance Officer. Their accountability for administration and compliance helps to ensure that all technical and behavioral firewalls are functioning as necessary.

8. B. (1) Monitoring efforts are accomplished through several vehicles. One mechanism involves the use of Highmark Health's data loss prevention (DLP) software-based monitoring tool. This DLP software was customized to perform, among other things, data sharing surveillance consistent with commonly accepted antitrust prevention standards. Through email fingerprinting designed to look for certain prescribed CSI terms and conditions, the DLP tool provides Highmark Health and its Entities purposive and systematic monitoring of email activity between Entities.

In the event that the DLP identifies email traffic containing certain documents which include CSI, or other unique contact identifiers containing CSI, the email delivery attempt is aborted. The specific email is quarantined and the sender is notified that the email is suspended until the CSI is removed. Contemporaneously, the Chief Privacy Officer will receive notice of the undelivered email through Infomgmtdecisions@highmarkhealth.org. The Chief Privacy Officer will commence any necessary investigation into the matter. In the event that a violation of CSI occurred or was intended to occur, necessary and appropriate remediation, mitigation and disciplinary steps will be taken that are consistent with Policy and the Order.

8. B. (2) Monitoring efforts also include management of current system access privileges and rights assigned to Personnel from both Entities. Unnecessary access rights are removed. Necessary and appropriate access privileges, particularly those associated with Personnel who have access to systems attributed to both Entities, are monitored. Email traffic is monitored, and any questionable or suspicious traffic containing CSI will be reported to the Chief Privacy Officer at Infomgmtdecisions@highmarkhealth.org. and an investigation will begin.

8. B. (3) Monitoring behavioral compliance with Policy is accomplished through after-hours clean desk walkthroughs of business areas that contain or are recognized as having appropriate access to CSI. These walkthroughs are part of Entities' general HIPAA-compliance activities but with an additional focus on CSI. The walkthroughs assist in observing current safeguards and developing additional safeguards and practices to ensure that access to CSI is proper controlled and protected. In the event that areas are found to have unsecure CSI, a corrective action plan is written and distributed to all stakeholders associated with that business area.

8. B. (4) Commencing with the Effective Date and consistent with the terms of the Policy and Order, Highmark Health developed and implemented an audit program to ensure controls are in place for the protection of CSI. The audit program will further audit the monitoring efforts identified and described in 8.B(2) above. Additionally, the audit verifies that Policies and all supporting procedures are followed. At a minimum, audits are conducted annually. All audit findings and observations are reported to the Chief Privacy Officer for investigation, remediation and reporting to the Audit Committee of the Board of Directors.

There were no material findings reported from the Effective Date through and including April 27, 2014.

8. C. Incident, Violations and Enforcement

Prior to the Effective Date of the Policy, and in anticipation of the Department approval, processes were established to report suspected violations of the proposed policy draft. As of the Effective Date, formal processes supporting incident reporting and enforcement were implemented and in effect.

8. C.(1) Incident and Violations

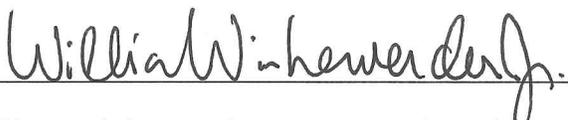
Consistent with the terms and conditions of the Order, and Policies, all Personnel are required to immediately report actual or suspected violations of Policy to the Chief Privacy Officer or other appropriate Director of Privacy, Senior Privacy Official.³ Personnel may report violations in confidence without fear of retribution or retaliation by: 1) contacting the Chief Privacy Officer via email to infomgmtdecisions@highmarkhealth.org; 2) by calling a toll-free hotline number provided in each Policy; or 3) by contacting the Director of Privacy or Senior Privacy Official directly.

There were no reported or otherwise known violations of Policy/Policies during the period⁴ covered by this Certification.

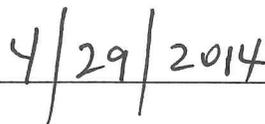
Condition 9 - Disclosure to Department

Entities agree to provide Department with such information regarding this Certification or any provision relating to it or the Policy/Policies referenced hereunder consistent with the terms and provisions of Condition 9. There are no corrective action plans to disclose to Department during the period covered by this Certification.

The undersigned acknowledge, agree and hereby certify that the representations made hereunder are true to the best of our knowledge, information and belief as of this date:



William Winkenwerder, Jr. CEO and President



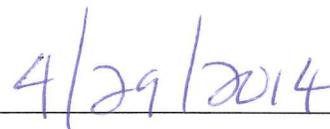
Date

Highmark Health

Date



Lisa A. Martinelli, Chief Privacy Officer



Date

Highmark Health

Date

¹ An amended and updated Attachment A reflecting organizational changes and new entities created since the Effective Date is attached hereto.

² Employees working in San Antonio, Texas eyewear laboratories do not have access to any data whatsoever and were not required to complete the training.

³ For the period covered by this Certification, reports made to Chief Privacy Officer or other PO consisted of emails accidentally sent to one entity or another that were determined not to contain CSI.

⁴ From the Effective Date through April 27 2014



EXHIBIT A
HIGHMARK INC. COMPANIES

1. Highmark Inc.
 - a. United Concordia Companies, Inc.
 - i. United Concordia Life and Health Insurance Company
 - ii. United Concordia Dental Plans of Pennsylvania, Inc.
 - b. Davis Vision, Inc.
 - i. DavisVision IPA, Inc.
 - c. HVHC Inc.
 - i. VisionWorks of America, Inc.
 1. VisionWorks, Inc.
 2. VisionWorks Enterprises, Inc.
 3. Empire Vision Center, Inc.
 - d. Highmark Select Resources Inc.
 - e. Keystone Health Plan West, Inc.
 - f. HM Life Insurance Company
 - g. HM Health Insurance Company
 - h. Highmark Senior Health Company (pending receipt of Certificates of Authority)
 - i. Highmark Coverage Advantage Inc. (pending receipt of Certificates of Authority)
 - j. Highmark Benefits Group Inc. (pending receipt of Certificates of Authority)

ALLEGHENY HEALTH NETWORK COMPANIES

1. HMPG Inc.
 - a. Promedix LLC
2. West Penn Allegheny Health System, Inc.
 - a. Alle-Kiski Medical Center
 - b. Canonsburg General Hospital
 - i. Canonsburg General Hospital Ambulance Service
 - c. Allegheny Medical Practice Network
 - d. Allegheny Clinic (f/k/a Allegheny Specialty Practice Network)
 - i. Physician Landing Zone
 1. Lake Erie Medical Group PC
 2. Premier Medical Associates, PC
 - e. West Penn Allegheny Oncology Network

3. Jefferson Regional Medical Center

- a. Prime Medical Group PCG 1
- b. Primary Care Group 2, Inc.
- c. Primary Care Group 3, Inc.
- d. Primary Care Group 4, Inc.
- e. Primary Care Group 5, Inc.
- f. Primary Care Group 6, Inc.
- g. Primary Care Group 7, Inc.
- h. Primary Care Group 8, Inc.
- i. Primary Care Group 9, Inc.
- j. Primary Care Group 10, Inc.
- k. Primary Care Group 11, Inc.
- l. Primary Care Group 12, Inc.
- m. Family Practice Medical Associates South, Inc.
- n. JRMC-Diagnostic Services, LLC
- o. Jefferson Magnetic Resonance Imaging, LLC
- p. The Park Cardiothoracic and Vascular Institute
- q. Specialty Group Practice 1, Inc.
- r. Grandis, Rubin, Shanahan & Associates
- s. Steel Valley Orthopaedic and Sports Medicine
- t. Jefferson Hills Surgical Specialists
- u. JRMC Specialty Group Practice
- v. JRMC Physician Services Corporation
- w. Pittsburgh Bone, Joint & Spine, Inc.

4. Saint Vincent Health Center

- a. Regional Heart Network

5. Saint Vincent Health System

- a. Clinical Services, Inc.
 - i. Saint Vincent Rehab Solutions, LLC
 - ii. Saint Vincent Consultants in Cardiovascular Diseases, LLC
 - iii. Saint Vincent NWPB Surgery Center, Ltd.
- b. Saint Vincent Affiliated Physicians
- c. Saint Vincent Medical Education & Research Institute, Inc.