

Jack M. Stover
717 237 4837
jack.stover@bipc.com

409 North Second Street
Suite 500
Harrisburg, PA 17101-1357
T 717 237 4800
F 717 233 0852
www.bipc.com

May 1, 2017

RECEIVED
Corporate & Financial Regulation

MAY 01 2017

Pennsylvania
Insurance Department

VIA HAND DELIVERY

Joseph DiMemmo, CPA
Deputy Insurance Commissioner
Office of Corporate and Financial Regulation
Pennsylvania Insurance Department
1345 Strawberry Square
Harrisburg, PA 17120

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 Mr. DiMemmo:

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, relating to the Policy Protecting Competitively Sensitive Information.

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

Thank you for your consideration.

Very truly yours,



Jack M. Stover

JMS/gmt
Enclosure

cc: Lawrence J. Beaser, Esquire (via email: Beaser@BlankRome.com)
Patrick T. DeLacey (via email: pat.delacey@raymondjames.com)

To: Insurance Department of the Commonwealth of Pennsylvania
From: David L. Holmberg, CEO and President Highmark Health
Lisa A. Martinelli, Vice President, Chief Privacy Officer Highmark Health
Date: April 25, 2017
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 (Initial Effective Date).

This Policy and the approved Firewall Policies for each Highmark Health Provider or Health Care Insurer (Approved Sub Policy, or Policy), as defined by the Order and as set forth in Attachment A¹ of the Policy, remained in effect throughout all or some part of the compliance period of April 19, 2016 through April 17, 2017 (Compliance Period) of this report; depending upon their respective effective dates.

7. A. Development

On January 23, 2017 the Department approved updates to the Approved Parent Firewall and Approved Sub Firewall Policies. The updates reflected changes in entity names, and clarification of reporting timelines. There have been no waivers, or terminations of the Approved Firewall Policy and/or Approved Sub Policies to report to the Department.

Policies have been in full force and effect at all times during this Compliance Period since their respective effective dates, and are publicly available on their respective entity website.

When applicable, and unless otherwise noted on Attachment A, necessary and appropriate Board approvals were obtained formally adopting Policies.

Condition 8 - Compliance with Policy

At all times during this Compliance Period, 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 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). In accordance with the Policy, the Highmark Health Privacy Department developed a formal training module for use when onboarding 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 cards contain 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 distributed prior to the Initial Effective Date and continue to be distributed to Personnel.

In addition to onboarding training, annual refresher training was provided to Personnel during the Compliance Period. Personnel who have access to CSI were required to participate in online privacy and security refresher training that included a detailed CSI component. Personnel were further required to certify that they completed the training, that they have accessed, read and understand the Policy, and they agree to abide by it.

From the period of April 19, 2016 through April 17, 2017, all forty-nine thousand six hundred and three (49,603) individual personnel who have access to Competitively Sensitive Information (Personnel) completed either onboarding or refresher training modules covering CSI. All Personnel acknowledged and agreed, 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

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

Supplemental targeted training was provided by the Chief Privacy Officer or her designee at the request of business units or management. This supplemental training continues to be provided from time to time at the request of management.

Refresher training was provided to members and directors of all Boards who are expected to comply with the Policy. Onboarding training was provided to newly appointed members and directors. Members and directors who are required to comply acknowledged and agreed through paper or online certification that they completed the training; that they read the Policy, have access to a copy of the Policy, understand the Policy and agree to abide by it. The Audit Committees of the Boards were periodically apprised of the monitoring and Policy compliance activities during the Compliance Period.

8. A. (2) Subsequent to the Initial 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 the Policy. The process also provides formal opportunities for Personnel who are uncertain if a particular use of data might potentially violate the Policies to bring their question to a subject matter expert for review and analysis. This process continued unabated throughout Compliance Period.

To ensure that proposed data sharing does not implicate or violate the 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, deny or appropriately modify 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.

The CSI Firewall Committee reviewed fifty-eight (58) requests for data sharing during the Compliance Period. Thirty-seven (37) of the requests were determined to be necessary and appropriate uses of data for treatment, payment and/or health plan operation purposes and did not constitute inappropriate uses of CSI. Five (5) requests were denied, seven (7) were withdrawn, it was determined that four (4) requests did not involve CSI and were received in error, and five (5) requests are still open pending review.

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 the Policy during this Compliance Period. This review and certification further represents that CSI was not used for any inappropriate purpose including disadvantaging rival competitor

Health Care Providers or Health Care Insurers during the Compliance Period. 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 Initial Effective Date, processes for monitoring compliance with the Policy were developed and implemented and have continued unabated throughout the Compliance Period. 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 contract 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 contract 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.

DLP monitoring continued unabated throughout the Compliance Period and did not detect any unauthorized uses of CSI in violation of this policy.

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.

Access monitoring efforts did not reveal any material incidents during the Compliance Period.

8. B. (3) Monitoring behavioral compliance with the 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 expanded 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 Initial 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 audited 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.

Fieldwork supporting this audit function commenced January 9, 2017 and was completed on April 17, 2017. There were no material audit findings reported during the Compliance Period.

Audits of the repository email address Infomgmtdecisions@highmarkhealth.org were additionally performed in order to review the data request processes described more fully in 8.A.(2). There were no material findings reported during the Compliance Period.

8. C. Incident, Violations and Enforcement

Prior to the Initial Effective Date of the Policy, processes were established to report suspected violations of the proposed policy draft. These formal processes supporting incident reporting and enforcement have continued unabated throughout the Compliance Period.

8. C. (1) Incident and Violations

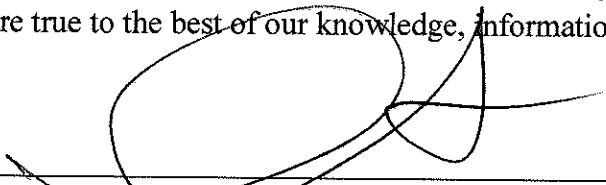
Consistent with the terms and conditions of the Order and Policies, all Personnel are required to immediately report actual or suspected violations of the Policy to the Chief Privacy Officer, appropriate Director of Privacy or Senior Privacy Official. Personnel may report violations in confidence without 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 Compliance Period.

Condition 9 - Disclosure to Department

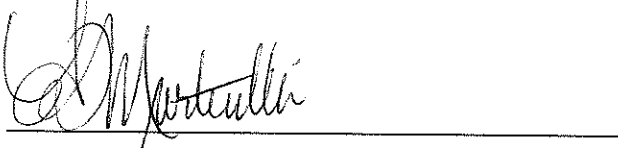
Entities agree to provide the Department with such information regarding this Certification or any provision relating to it or the Policy/Policies referenced hereunder consistent with the terms and provisions of Condition 9. There are no corrective action plans to disclose to the Department during the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



David L. Holmberg, CEO and President

Highmark Health

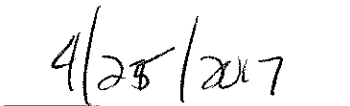


Lisa A. Martinelli, Vice President, Chief Privacy Officer

Highmark Health



Date



Date

¹ An amended and updated Attachment A reflecting organizational changes and new entities created during this Compliance Period 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.

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. Highmark Choice Company
 - f. HM Life Insurance Company
 - g. HM Health Insurance Company
 - h. Highmark Senior Health Company
 - i. Highmark Coverage Advantage Inc.
 - j. Highmark Benefits Group Inc.
 - k. HM Centered Health Inc.

ALLEGHENY HEALTH NETWORK COMPANIES

1. HMPG Inc.
 - a. Promedix LLC
 - b. Klingensmith, Inc.
 - c. Monroeville ASC LLC
 - d. Physician Partners of Western PA 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
 - i. Physician Landing Zone, PC
 1. Lake Erie Medical Group PC
 2. Premier Medical Associates, PC

- ii. Premier Women's Health
 - e. JV Holdco, LLC
 - f. Allegheny Clinic Medical Oncology
 - g. Peters Township Surgery Center, LLC
- 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 10, Inc.
 - j. Primary Care Group 11, Inc.
 - k. Primary Care Group 12, Inc.
 - l. Family Practice Medical Associates South, Inc.
 - m. JRMC Diagnostic Services, LLC
 - n. The Park Cardiothoracic and Vascular Institute
 - o. Grandis, Rubin, Shanahan & Associates
 - p. Steel Valley Orthopaedic and Sports Medicine
 - q. Jefferson Hills Surgical Specialists
 - r. JRMC Specialty Group Practice
 - s. JRMC Physician Services Corporation
 - t. Pittsburgh Bone, Joint & Spine, Inc.
 - u. Pittsburgh Pulmonary and Critical Care Associates
 - v. South Pittsburgh Urology Associates
- 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 NWPA Surgery Center, Ltd.
 - b. Saint Vincent Affiliated Physicians
 - c. Saint Vincent Medical Education & Research Institute, Inc.
 - d. Allegheny Health Network Home Infusion, LLC