pennsylvania
INSURANCE DEPARTMENT

October 24, 2013

Jack M. Stover, Esquire
Buchanan Ingersoll & Rooney PC
409 North Second Street, Suite 500
Harrisburg, PA 17101-1357

RE: The Proposed Highmark Firewall Policies Protecting Competitively Sensitive Information Submitted in Response to Condition 7 of the Approving Determination and Order (Order No. ID-RC-13-06)

Dear Mr. Stover:

The Pennsylvania Insurance Department's Approving Determination and Order (Order No. ID-RC-13-06) (the "Order")[1] required that Highmark ". . . file with the Department, for the review and Approval of the Department, a comprehensive Firewall Policy . . . ." Highmark timely filed its proposed Firewall Policy.[2] Since that time, the Pennsylvania Insurance Department ("the Department") has reviewed that filing to ensure that the proposed Firewall Policies meet all of the Order's requirements.

In response to comments from the Department's consultants, on October 4, 2013 Highmark submitted for approval a revised version of the proposed "Policies Protecting Competitively Sensitive Information for Highmark and other entities within its delivery system" (the "Proposed Firewall Policies"). The submission included two separate policies, one for Highmark and one for the other entities included on the list in Attachment A to each Proposed Firewall Policy.

Background

The purpose of the Firewall Policy, as stated in Appendix 2 of the Order ("Appendix 2"), is to "avoid the inadvertent or intentional disclosure of Competitively Sensitive Information that could potentially reduce substantially competitive innovation or pricing between and/or among the vertically integrated entities and their rivals at the provider and insurer levels."

Common ownership of the Domestic Insurers and the WPAHS Entities provides the opportunity for each to obtain and make use of Competitively Sensitive Information from rivals that could be used to the potential detriment of consumers and competition. A risk to competition exists if a Domestic Insurer can adversely affect any rival's price and non-price contract terms or deter innovation or access or limit gains to innovation by obtaining and acting upon any rival's Competitively Sensitive Information.

Condition 7 requires that the Proposed Firewall Policies be "in a form and substance acceptable to the Department" and that they be submitted "for review and Approval of the Department." For purposes of Condition 7, the term "Approval of the Department" means ". . . when the Department expressly grants its written approval to a written request by the applicable requesting party for Department approval."[3] Once approved, the firewall policies are required to be made "publicly available in accordance with the requirements of the Department."

[1] See: http://www.portal.state.pa.us/portal/server.pt/community/industry_activity/9276/highmark_west_penn_allegheny_health_system/982185

[2] Terms used in this letter generally have the same meaning as defined in the Order. For example, see the definition of "Firewall Policy" in Appendix 1 (Definitions) of the Order ("Appendix 1"). However, "UPE" will be referred to in this letter as "Highmark."

[3] See Order, definition of "Approval of the Department."

Approval and Implementation

It is incumbent upon Highmark to assure that each of the Proposed Firewall Policies is fully implemented and rigorously enforced, as required by the Order. If so, the Proposed Firewall Policies should mitigate the competitive concerns discussed above and should be effective in maintaining competition in the health care insurance and provider services markets by ensuring the confidentiality of Competitively Sensitive Information. Moreover, the Department believes that the Proposed Firewall Policies provide a sound model that should be considered for adoption by other integrated health care firms offering both health insurance and hospital and physician provider services to consumers.

Therefore, the Department hereby approves each of the Proposed Firewall Policies submitted to the Department on October 4. The approval is subject to the understanding of the Department that the Proposed Firewall Policies will be fully implemented and vigorously enforced, and the Department reserves the right to require changes to the Proposed Firewall Policies if, as a result of the implementation, the objectives of Condition 7 are not being met.

Under the terms of Condition 7, once approved, the Firewall Policies must be "made publicly available in accordance with the requirements of the Department." The Department will post the Firewall Policies on its public website and requires that each of the entities listed in Attachment A of the Firewall Policies make a copy of the applicable Firewall Policy easily available to the public by posting the full text on each entity's website.

Sincerely,

Stephen J. Johnson, CPA
Deputy Insurance Commissioner
Office of Corporate and Financial Regulation

Policy Protecting Competitively Sensitive Information

I. Scope

Highmark adopts this Policy Protecting Competitively Sensitive Information (CSI) and will require each of the Highmark Health Companies and AHN Companies designated on Attachment A to this Policy, collectively referred to as the "System," to adopt a CSI Policy that is consistent with the terms of this Policy. All System Personnel, including all directors, officers, other employees, trainees, volunteers, and independent contractors are subject to and shall *strictly* comply with this Policy.

II. Purpose

The Pennsylvania Insurance Department ("Department") has raised the concern that the corporate affiliation of Highmark Health Services companies (as buyers of healthcare medical services), Allegheny Health Network companies (as sellers of healthcare medical services), and Highmark (as the parent company) could result in one or more of these entities obtaining or sharing information on the terms and conditions of rival contracts. The Department expressed concern that the result could be a reduction in competition, competitive innovation or pricing between the now affiliated companies and their rivals at one or more levels. To prevent such potential adverse competitive effects, the Department requires that the System develop, implement and strictly comply with Firewalls to restrict Highmark Health Services companies' knowledge of and ability to influence Allegheny Health Network companies' negotiations with rival insurers. Similarly, development, implementation and strict compliance with Firewalls is required to restrict Allegheny Health Network companies' influence on Highmark Health Services companies' negotiations with rival hospitals.

Accordingly, Highmark has determined that the adoption of this Policy throughout the System will serve to protect CSI against inappropriate access, use or disclosure, as required as a condition of the Department's Approving Determination and Order issued on May 29, 2013, Order No. ID-RC-13-06. This Policy is implemented and will be enforced in accordance with the Department's Approving Determination and Order. A copy of that Order may be found at *http://www.portal.state.pa.us/portal/server/pt/community/industry_activity/9276/application_materials/1014652*. This Policy sets forth the requirements and processes to safeguard

against such inappropriate access, use or disclosure of CSI between and among companies within the System and their respective Personnel.

The policy is not intended to replace Highmark Policy 132, titled "Information Use, Management and Disclosure," but to supplement it, particularly with respect to the imposition of procedures to accomplish the objectives of that Policy. To the extent that there are inconsistencies between this Policy and Highmark Policy 132, the provisions of this Policy shall control and supersede the provisions of Highmark Policy 132.

III. Definitions

A. ***Competitively Sensitive Information (CSI)*** protected under this Policy includes the following categories of non-public information held by the System: Past, present and future reimbursement rates and rate schedules; contracts with providers; contracts with payers; any term or condition in a payer-provider agreement that could be used to gain an unfair commercial advantage over a competitor or supplier, including but not limited to discounts, reimbursement methodologies, and provisions relating to performance, pay for performance, pay for value, tiering of providers, cost data and methodologies including specific cost and member information and revenue, or discharge information specific to the payer or provider; contract negotiations or negotiating positions, including but not limited to offers, counteroffers, party positions, and thought processes; specific plans regarding future negotiations or dealings with payers or providers; and claims reimbursement data.

B. ***Firewalls*** refer to safeguards that restrict unauthorized access, use and sharing of CSI. Firewalls segregate and protect CSI through procedures, training and behavioral guidelines and processes applicable to all System Personnel in their interactions with one another. Firewalls also include software-based and hardware-based tools and equipment to protect CSI and create additional barriers to unauthorized access. Firewalls prohibit the sharing of CSI in any form, whether oral, written, electronic or otherwise.

C. ***Highmark*** is the parent entity of both Highmark Health Services and Allegheny Health Network.

D. ***Highmark Health Services (Highmark Health)*** is a subsidiary of Highmark. Highmark Health and the companies it controls conduct the insurance business of the System. The Highmark Health companies identified on Attachment "A" are referred to in this Policy as the "Highmark Health Companies".

E. ***Allegheny Health Network (AHN)*** is a subsidiary of Highmark. AHN and the companies it controls conduct the provider services of the System. The AHN companies identified on Attachment "A" are referred to in this Policy as the "AHN Companies".

F. ***System*** is the collective reference to Highmark, Highmark Health and AHN.

G. ***Personnel*** includes any director, officer, other employee, trainee, volunteer, independent contractor or consultant performing services on behalf of the System or any company within the System.

IV. Roles and Responsibilities

A. Highmark's Chief Executive Officer, President and Board of Directors shall be ultimately accountable and responsible for the adoption, implementation, monitoring and strict enforcement of this Policy. The Audit Committee of the Board shall require periodic reports regarding compliance with this Policy and shall report that information to the full Board.

B. Subject to A above, the following shall be responsible for administration of this Policy:

1. Chief Privacy Officer, Highmark
2. Chief Auditor and Compliance Officer, Highmark
3. Chief Legal Officer, Highmark
4. Chief Information Security Officer, Highmark Health Services
5. Chief Information Security Officer, Allegheny Health Network

V. Policy and Administration

A. All Personnel must strictly observe the following Policy to protect against the inappropriate access, use or disclosure of CSI:

1. Highmark Personnel who have access to, or are in possession of, any CSI of any Highmark Health Company shall not disclose such CSI to any AHN Company or any of its Personnel.

   Example: *While reviewing Highmark Health's audit findings of a non-affiliated hospital's billing practices, Alice, Highmark's Chief Auditor and Compliance Officer, sees reports that contains the hospital's reimbursement and rate schedules. Alice is prohibited from disclosing this CSI to any AHN Personnel.*

2. Highmark Personnel who have access to, or are in possession of, any CSI of any AHN Company shall not disclose such CSI to any Highmark Health Company or any of its Personnel;

   Example: *While reviewing the audit findings of an AHN provider's billing practices, Alice, Highmark's Chief Auditor and Compliance Officer, sees reports that contain reimbursement and rate schedules from other insurance carriers. Alice is prohibited from disclosing this CSI to any Highmark Health Personnel.*

3. AHN Personnel who have access to or are in possession of any CSI of any AHN Company shall not disclose such CSI to any Highmark Health Company or any of its Personnel;

   Example: *John is Associate Counsel at AHN and one of his responsibilities is to negotiate the terms and conditions of third party payer contracts. After a long and protracted series of negotiations, John successfully reaches a good deal for AHN physicians, and concludes the contract negotiation with Acme Health Insurer. That afternoon, John has lunch with his friend Ben who works at Highmark Health. John cannot discuss the negotiations, his thoughts and impressions, and the results of the negotiation with Ben because sharing the information would violate this Policy and compromise Competitively Sensitive Information.*

4. Highmark Health Personnel who have access to or are in possession of any CSI of any Highmark Health Company shall not disclose such CSI to any AHN Company or any of its Personnel.

   Example: *Mabel works as an account service manager in the National Accounts area of Highmark Health. In providing plan administration reports to her self-funded group accounts, Mabel regularly sees claims reimbursement and utilization reports for unaffiliated providers who treat members of the group account. Mabel rides the bus everyday with Sandy who works in Physician Services for AHN and is responsible for assisting in the recruitment of new physicians into the network. During their ride to work one morning, Sandy asks Mabel if she could research a particular physician practice and share their patient utilization and reimbursement information with her so that she can determine if they are a good recruiting target. Mabel is prohibited from sharing any of the billing, claims reimbursement and utilization reports of Highmark Health unaffiliated providers with Sandy because it is CSI.*

B. All Personnel must take mandatory CSI Policy training and all newly-hired Personnel must do so before performing any work for the System. There will be no exceptions to this mandatory requirement. The System shall provide periodic refresher training regarding the protection of CSI, at least annually, and supplemental training as necessary. CSI Policy training shall be developed, designed, facilitated and administered by the Highmark Chief Privacy Officer. At the completion of the mandatory training session and after each refresher training session, all Personnel shall be required to certify completion of the program and comprehension of the materials presented.

C. All Personnel must excuse themselves from participation in any activity where their participation would necessarily involve the improper access, use or disclosure of CSI. Any individual who comes in contact with CSI from either Highmark Health or AHN in the ordinary course of his or her job function cannot use that CSI in performing any activity or service for the other company. If that activity requires sharing or reference to the CSI, the individual must excuse himself or herself from that activity.

   Example: *James is an executive of Highmark and also serves as a director of AHN. In his executive position and in the course of his job function he properly receives CSI from Highmark Health regarding recent rate negotiations with Hospital A, a competitor of AHN. At the next AHN board meeting, James must not disclose that CSI and must excuse*

himself from AHN board discussions or actions that would involve the use or disclosure of that CSI.

D. All Personnel are encouraged to contact the Highmark Chief Privacy Officer if they have any questions about their responsibilities or other matters pertaining to this Policy.

VI. Infrastructure and Physical Safeguards

A. The System shall continue to observe current safeguards and adopt any additional safeguards sufficient to assure that access to CSI is properly controlled and protected. Such safeguards include:

- Role based access
- Control and Management of User IDs
- Separation of servers or data stored on servers as appropriate
- Monitoring systems for unauthorized access
- Other necessary technical controls to accomplish segregation of duties, businesses and roles.

B. The System shall continue to use security tools that include electronic interface with the Human Resources systems to provide information regarding the identity of authorized Personnel in each business area, including updates on terminations, new hires, transfers and other position and organization changes.

C. Strong PC/workstation controls shall continue to protect CSI from unauthorized access or transmission.

VII. Monitoring and Auditing

A. The Highmark Privacy Department shall be responsible for monitoring the System to assure that CSI has not been inappropriately accessed, used or disclosed.

B. Highmark's Internal Audit Department shall develop and implement an audit plan to assure that proper controls are in place for the protection of CSI and that all policies and procedures are followed. Internal Audit shall conduct regular audits of the System to ensure compliance with this Policy. Audit findings and observations shall be reported to the Highmark Chief Privacy Officer for appropriate remediation and mitigation, and ultimately reported to the Audit Committee of the Board of Directors.

C. All Personnel shall certify annually that they have read and understood this Policy and that they are in full compliance with it. In addition, all Personnel shall certify their responsibility to report actual or potential violations with the understanding that such reporting will not result in retribution or retaliation by any company or Personnel within the System. Highmark's Internal Audit Department shall monitor these annual certifications to insure compliance with this Policy.

D. All Personnel shall also affirmatively acknowledge that failure to report an actual or potential violation of this Policy may subject the individual to disciplinary action, up to and including termination.

VIII. Violations and Enforcement

A. Violations of this Policy are subject to corrective action up to and including termination of employment or contractual arrangement, or removal from the Board, consistent with System disciplinary procedures.

B. All Personnel are required to immediately report violations or suspected violations of this Policy to the Highmark Chief Privacy Officer and to the Privacy Officer assigned to their company where different. The Highmark Chief Privacy Officer or others acting under his or her direction shall investigate and take appropriate remedial action including determining the cause(s) of any violation, mitigating the effects of the violation, taking corrective action to prevent future occurrences, and engaging Highmark Human Resource areas as necessary to determine appropriate sanctions.

Example: *Tricia, a data analyst in the AHN provider financial operations area sits in the cubicle next to her colleague Glen. One afternoon Tricia overhears Glen talking on the phone to Helen who works as an analyst in Highmark Health Informatics. Glen thanks Helen for the report she generated and sent to him containing Highmark BCBS member-level data pertaining to specific cost and reimbursement rates for particular drugs and the associated prescribing provider information. Concerned that competitively sensitive information was compromised, Tricia contacts the Highmark Chief Privacy Officer.*

C. In any case in which any individual has violated or is suspected to have violated this Policy, the Highmark Chief Privacy Officer will notify Highmark Human Resources and provide case-specific information to enable Highmark Human Resources and the

business unit management to administer appropriate disciplinary measures. In any case in which a director or executive officer has violated or is suspected to have violated this Policy, the Highmark Chief Privacy Officer shall notify the Personnel and Compensation Committee of the Board, which may appoint a director or other designee to assist and participate in the investigation. If a violation is found, the Board shall discipline the director or officer as it deems appropriate. There is zero tolerance for intentional improper access, use or disclosure of CSI in violation of this Policy.

D. Failure to report known or suspected violations of this Policy shall constitute a violation.

IX. Filing a Complaint

A. Complaints or reports may be made in any of the following ways:

(1) directly to the Highmark Chief Privacy Officer,

(2) by calling toll-free: 1-877-959-4160,

(3) or by email to *infomgmtdecisions@highmark.org.*

B. The Highmark Privacy Department, including the privacy officers for companies listed on Attachment A, shall have responsibility for administrative enforcement of this Policy and shall promptly investigate and ensure that necessary and appropriate remedial action is taken in response to all reported violations. The remedial actions taken shall include determination of the cause(s) of the violation, mitigation, corrective action that is required to prevent future occurrences, and facilitating appropriate workforce sanctioning if applicable.

X. Policy Against Retaliation

The System is committed to protecting all Highmark Personnel, health care providers with whom any Highmark Health Services company contracts, and members of the general public (collectively referred to as "Individuals") from interference with making a good faith disclosure that this Policy has been violated, from retaliation for having made a good faith disclosure, or from retaliation for having refused a direction or order in conflict with this Policy. The System encourages all Individuals to report good faith concerns about a potential violation of this Policy. No Individual or entity who in good faith reports a violation of this Policy, or who participates in the investigation of a reported violation of this Policy, will suffer harassment, retaliation, adverse employment or other adverse action as a result of the

Individual's report and/or participation. Any System Personnel who retaliates against someone who has reported a violation of this Policy in good faith, or who has participated in an investigation of a reported violation, is subject to discipline up to and including termination of employment or contractual arrangement or removal from the Board.

> Example: *Community Hospital A, in attempting to negotiate its provider contract with Highmark Health Services has evidence that Highmark Health Services knows the terms and conditions of Community Hospital A's provider contract with other insurers. In the event that Community Hospital A files a complaint against Highmark Health Services, Highmark Health Services may not take any negative action with respect to its relationship with Community Hospital A as a result of this complaint.*

> Example: *Kathleen works at West Penn Hospital where as part of her duties, she gathers materials to assist the team that negotiates the hospital's rates with insurers. As she is preparing information about the hospital's recent experience providing services to subscribers of National Insurer, she finds an email from her supervisor to an employee of Highmark Health Services attaching West Penn's current agreement with National Insurer. Kathleen reports her findings to the Highmark Chief Privacy Officer, which triggers an investigation and results in serious discipline of her supervisor. Neither the supervisor nor any other System Personnel may take any negative action toward Kathleen for complying with her obligations under this Policy.*

XI. No Exceptions

There are no exceptions to this Policy regarding improper access, use or disclosure of CSI.

XII. HIPAA Compliance

Nothing in this Policy is intended to prohibit or otherwise prevent disclosure of information that may include competitively sensitive data elements if the disclosure is necessary, appropriate and required to comply with the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under HITECH, GINA and other modifications to the HIPAA Rules as set forth in 45 CFR Parts 160 and 164.

XIII. Amendments

Any amendments to this Policy are subject to approval by the Pennsylvania Insurance Department.

ATTACHMENT A

Highmark shall report any changes to this Attachment A to the Pennsylvania Insurance Department within 5 business days of that change.

HIGHMARK

HIGHMARK HEALTH SERVICE COMPANIES

1. Highmark Health Services
    a. United Concordia Companies, Inc.
        i. United Concordia Life and Health Insurance Company
        ii. United Concordia Dental Plans of Pennsylvania, Inc.
    b. HVHC Inc.
        i. VisionWorks, Inc.
        ii. VisionWorks Enterprises, Inc.
        iii. Empire Vision Center, Inc.
    c. Highmark Senior Resources Inc.
    d. Keystone Health Plan West, Inc.
    e. HM Life Insurance Company
    f. HM Health Insurance Company

ALLEGHENY HEALTH NETWORK COMPANIES

1. Allegheny Health Network
    a. HMPG Inc.
        i. Promedix LLC
        ii. Physician Landing Zone PC
            1. Lake Erie Medical Group PC
            2. Premier Medical Associates, PC

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 Specialty Practice Network
    e. West Penn Allegheny Oncology Network
    f. West Penn Physician Practice 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
    b. Erie Regional DMAT PA-3

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.

6. Highmark Health Services
    a. Davis Vision, Inc.
        i. DavisVision IPA, Inc.

DIVIDER PAGE

Policy Protecting Competitively Sensitive Information

I. Scope

[Sub] adopts and is ultimately responsible and accountable for the administration and enforcement of this Policy Protecting Competitively Sensitive Information (CSI) in compliance with the Highmark Policy Protecting Competitively Sensitive Information for the Highmark System as defined in that policy and including all companies designated on Attachment A to this Policy. All **[Sub]** Personnel, including all directors, officers, other employees, trainees, volunteers, and independent contractors are subject to and shall strictly comply with this Policy.[1]

II. Purpose

The Pennsylvania Insurance Department ("Department") has raised the concern that the corporate affiliation of Highmark Health Services companies (as buyers of healthcare medical services), Allegheny Health Network companies (as sellers of healthcare medical services), and Highmark (as the parent company) could result in one or more of these entities obtaining or sharing information on the terms and conditions of rival contracts. The Department expressed concern that the result could be a reduction in competition, competitive innovation or pricing between the now affiliated companies and their rivals at one or more levels. To prevent such potential adverse competitive effects, the Department requires that the System develop, implement and strictly comply with Firewalls to restrict Highmark Health Services companies' knowledge of and ability to influence Allegheny Health Network companies' negotiations with rival insurers. Similarly, development, implementation and strict compliance with Firewalls is required to restrict Allegheny Health Network companies' influence on Highmark Health Services companies' negotiations with rival hospitals.

Accordingly, **[Sub]** has determined that the adoption of this Policy will serve to protect CSI against inappropriate access, use or disclosure, as required as a condition of the Department's Approving Determination and Order issued on May 29, 2013, Order No. ID-RC-13-06. This Policy is implemented and will be enforced in accordance with the Department's Approving

---

[1] Each adopting company will adjust this model policy only as necessary to reflect the organizational structure of that company.

Determination and Order. A copy of that Order may be found at *http://www.portal.state.pa.us/portal/server/pt/community/industry_activity/9276/application_materials/1014652*. This Policy sets forth the requirements and processes to safeguard against such inappropriate access, use or disclosure of CSI between and among companies within the System and their respective Personnel.

This Policy is not intended to replace Highmark Policy 132, titled "Information Use, Management and Disclosure," but to supplement it, particularly with respect to the imposition of procedures to accomplish the objectives of that Policy. To the extent that there are inconsistencies between this Policy and Highmark Policy 132, the provisions of this Policy shall control and supersede the provisions of Highmark Policy 132.

III. Definitions

A. ***Competitively Sensitive Information (CSI)*** protected under this Policy includes the following categories of non-public information held by the System: Past, present and future reimbursement rates and rate schedules; contracts with providers; contracts with payers; any term or condition in a payer-provider agreement that could be used to gain an unfair commercial advantage over a competitor or supplier, including but not limited to discounts, reimbursement methodologies, and provisions relating to performance, pay for performance, pay for value, tiering of providers, cost data and methodologies including specific cost and member information and revenue, or discharge information specific to the payer or provider; contract negotiations or negotiating positions, including but not limited to offers, counteroffers, party positions, and thought processes; specific plans regarding future negotiations or dealings with payers or providers; and claims reimbursement data.

B. ***Firewalls*** refer to safeguards that restrict unauthorized access, use and sharing of CSI. Firewalls segregate and protect CSI through procedures, training and behavioral guidelines and processes applicable to all System Personnel in their interactions with one another. Firewalls also include software-based and hardware-based tools and equipment to protect CSI and create additional barriers to unauthorized access. Firewalls prohibit the sharing of CSI in any form, whether oral, written, electronic or otherwise.

C. ***Highmark*** is the parent entity of both Highmark Health Services and Allegheny Health Network.

D. ***Highmark Health Services (Highmark Health)*** is a subsidiary of Highmark. Highmark Health and the companies it controls conduct the insurance business of the System. The Highmark Health companies identified in Attachment A are referred to in this Policy as "Highmark Health Companies."

E. ***Allegheny Health Network (AHN)*** is a subsidiary of Highmark. AHN and the companies it controls conduct the provider services of the System. The AHN companies identified in Attachment A are referred to in this Policy as "AHN Companies."

F. ***System*** is the collective reference to Highmark, Highmark Health and AHN.

G. ***Personnel*** includes any director, officer, other employee, trainee, volunteer, independent contractor or consultant performing services on behalf of the System or any company within the System.

H. ***[Sub] Personnel*** includes any director, officer, other employee, trainee, volunteer, independent contractor or consultant performing services on behalf of **[Sub]**.

I. ***Director of Privacy*** is the individual responsible for privacy oversight for AHN or Highmark Health respectively and who is directly accountable to the Highmark Chief Privacy Officer.

J. ***Senior Privacy Official*** is the **[Sub]** employee responsible for privacy oversight of the **[Sub]**.

IV. Roles and Responsibilities

A. **[Sub's]** President and Board shall be ultimately accountable and responsible for the adoption, implementation, monitoring and strict enforcement of this Policy. The Audit Committee of the Board, or those performing the audit function, shall require periodic reports regarding compliance with this Policy and shall report that information to the full Board.

B. Subject to A above, the following shall be responsible for administration of this Policy:

1. Director of Privacy, and/or Senior Privacy Official for **[Sub]**
2. [Senior Auditor and Compliance Officer, **Sub**]
3. [Senior Legal Officer, **Sub**]

4. [Senior Information Security Officer, **Sub**]

V. Policy and Administration

A. All **[Sub]** Personnel must strictly observe the following Policy to protect against the inappropriate access, use or disclosure of CSI:

1. **[Sub]** Personnel who have access to, or are in possession of, any CSI of any Highmark Health Company shall not disclose such CSI to AHN or to any Personnel of an AHN Company.

   Example: *Mabel works as an account service manager in the National Accounts area of Highmark Health. In providing plan administration reports to her self-funded group accounts, Mabel regularly sees claims reimbursement and utilization reports for nonaffiliated providers who treat members of the group account. Mabel rides the bus everyday with Sandy who works in Physician Services for AHN and is responsible for assisting in the recruitment of new physicians into the network. During their ride to work one morning, Sandy asks Mabel if she could research a particular physician practice and share their utilization and reimbursement information with her so that she can determine if they are a good recruiting target. Mabel is prohibited from sharing any of the billing, claims reimbursement and utilization reports of Highmark Health nonaffiliated providers with Sandy because it is CSI.*

2. **[Sub]** Personnel who have access to, or are in possession of, any CSI of any AHN Company shall not disclose such CSI to Highmark Health or to any Personnel of a Highmark Health Company;

   Example: *John is Associate Counsel at AHN and one of his responsibilities is to negotiate the terms and conditions of third party payer contracts. After a long and protracted series of negotiations, John successfully reaches a good deal for AHN physicians, and concludes the contract negotiation with Acme Health Insurer. That afternoon, John has lunch with his friend Ben who works at Highmark Health. John cannot discuss the negotiations, his thoughts and impressions, and the results of the negotiation with Ben because sharing the information would violate this Policy and compromise Competitively Sensitive Information.*

B. All **[Sub]** Personnel must take mandatory CSI Policy training and all newly-hired **[Sub]** Personnel must do so before performing any work. There will be no exceptions to this

mandatory requirement. **[Sub]** shall provide periodic refresher training regarding the protection of CSI, at least annually, and supplemental training as necessary. CSI Policy training shall be developed, designed, facilitated and administered by the Highmark Chief Privacy Officer. At the completion of the mandatory training session and after each refresher training session, all **[Sub]** Personnel shall be required to certify completion of the program and comprehension of the materials presented.

C. **All [Sub]** Personnel must excuse themselves from participation in any activity where their participation would necessarily involve the improper access, use or disclosure of CSI. Any individual who comes in contact with CSI from either Highmark Health or AHN in the ordinary course of his or her function cannot use that CSI in performing any activity or service for the other company. If that activity requires sharing or reference to the CSI, the individual must excuse himself or herself from that activity.

Example: *James is an executive of Highmark and also serves as a director of AHN. In his executive position and in the course of his job function he properly receives CSI from Highmark Health regarding recent rate negotiations with Hospital A, a competitor of AHN. At the next AHN board meeting, James must not disclose that CSI and must excuse himself from AHN board discussions or actions that would involve the use or disclosure of that CSI.*

D. All **[Sub]** Personnel are encouraged to contact the Highmark Chief Privacy Officer or **[Sub]** Director of Privacy or the Senior Privacy Official for **[Sub]** if they have any questions about their responsibilities or other matters pertaining to this Policy.

VI. Infrastructure and Physical Safeguards

A. **[Sub]** shall continue to observe current safeguards and adopt any additional safeguards sufficient to assure that access to CSI is properly controlled and protected. Such safeguards include:

- Role based access
- Control and Management of User IDs
- Separation of servers or data stored on servers as appropriate
- Monitoring systems for unauthorized access

- Other necessary technical controls to accomplish segregation of duties, businesses and roles.

B. **[Sub]** shall continue to use security tools that include electronic interface with the Human Resources systems to provide information regarding the identity of authorized **[Sub]** Personnel in each business area, including updates on terminations, new hires, transfers and other position and organization changes.

C. Strong PC/workstation controls shall continue to protect CSI from unauthorized access or transmission.

VII. Monitoring and Auditing

A. The Highmark Privacy Department shall be responsible for monitoring the System, including **[Sub]**, to assure that CSI has not been inappropriately accessed, used or disclosed.

B. Highmark's Internal Audit Department shall develop and implement an audit plan to assure that proper controls are in place for the protection of CSI and that all policies and procedures are followed. Internal Audit shall conduct regular audits of the System, including **[Sub]**, to ensure compliance with this Policy. Audit findings and observations shall be reported to the Highmark Chief Privacy Officer for appropriate remediation and mitigation, and ultimately reported to the Highmark Audit Committee, which shall report to the full Highmark Board, and to the Audit Committee of the **[Sub]** Board or those performing the audit function, who shall report to the full **[Sub]** Board.

C. All **[Sub]** Personnel shall certify annually that they have read and understood this Policy and that they are in full compliance with it. In addition, all **[Sub]** Personnel shall certify their responsibility to report actual or potential violations with the understanding that such reporting will not result in retribution or retaliation by any company or Personnel within the System. Highmark's Internal Audit Department shall monitor these annual certifications to insure compliance with this Policy. All annual certifications will be reported to Highmark's Chief Privacy Officer for inclusion in the annual report on System compliance.

D. All **[Sub]** Personnel shall also affirmatively acknowledge that failure to report an actual or potential violation of this Policy may subject the individual to disciplinary action, up to and including termination.

VIII. Violations and Enforcement

A. Violations of this Policy are subject to corrective action up to and including termination of employment or contractual arrangement, or removal from the Board, consistent with Highmark and **[Sub]** disciplinary procedures.

B. All **[Sub]** Personnel are required to immediately report violations or suspected violations of this Policy to the **[Sub]** Senior Privacy Official, who shall notify the appropriate Director of Privacy, who shall notify the Highmark Chief Privacy Officer. The Highmark Chief Privacy Officer, the appropriate Director of Privacy and the **[Sub]** Senior Privacy Official shall investigate and take appropriate remedial action including determining the cause(s) of any violation, mitigating the effects of the violation, taking corrective action to prevent future occurrences, and engaging Human Resource areas as necessary to determine appropriate sanctions.

Example: *Tricia, a data analyst in the AHN provider financial operations area sits in the cubicle next to her colleague Glen. One afternoon Tricia overhears Glen talking on the phone to Helen who works as an analyst in Highmark Health Informatics. Glen thanks Helen for the report she generated and sent to him containing Highmark BCBS member-level data pertaining to specific cost and reimbursement rates for particular drugs and the associated prescribing provider information. Concerned that competitively sensitive information was compromised, Tricia contacts the Highmark Chief Privacy Officer.*

C. In any case in which any individual has violated or is suspected to have violated this Policy, the **[Sub]** Senior Privacy Official, the appropriate Director of Privacy and the Highmark Chief Privacy Officer shall notify **[Sub]** Human Resources and provide case-specific information to enable **[Sub]** Human Resources and **[Sub]** business unit management to administer appropriate disciplinary measures. In any case in which a director or executive officer of **[Sub]** has violated or is suspected to have violated this Policy, the **[Sub]** Senior Privacy Official shall notify the appropriate Director of Privacy, who shall notify the Highmark Chief Privacy Officer, who shall oversee the investigation. If a violation is found, the Board with appropriate authority shall discipline the director or officer as it deems appropriate. There is zero tolerance for intentional improper access, use or disclosure of CSI in violation of this Policy.

D. Failure to report known or suspected violations of this Policy shall constitute a violation.

IX. Filing a Complaint

A. Complaints and reports may be made in any of the following ways:

(1) directly to the **[Sub]** Senior Privacy Official or the Highmark Chief Privacy Officer,

(2) by calling toll-free: 1-877-959-4160,

(3) or by email to infomgmtdecisions@highmark.org.

B. The Highmark Chief Privacy Officer shall have ultimate responsibility for the administrative enforcement of this Policy. The Highmark Chief Privacy Officer, the appropriate Director of Privacy and the **[Sub]** Senior Privacy Official shall promptly investigate and ensure that necessary and appropriate remedial action is taken in response to all reported violations. The remedial actions taken shall include determination of the cause(s) of the violation, mitigation, corrective action that is required to prevent future occurrences, and facilitating appropriate workforce sanctioning if applicable.

X. Policy Against Retaliation

[Sub] is committed to protecting all Personnel, health care providers with whom any Highmark Health Services company contracts, and members of the general public (collectively referred to as "Individuals") from interference with making a good faith disclosure that this Policy has been violated, from retaliation for having made a good faith disclosure, or from retaliation for having refused a direction or order in conflict with this Policy. **[Sub]** encourages all Individuals to report good faith concerns about a potential violation of this Policy. No Individual or entity who in good faith reports a violation of this Policy, or who participates in the investigation of a reported violation of this Policy, will suffer harassment, retaliation, adverse employment or other adverse action as a result of the Individual's report and/or participation. Any **[Sub]** Personnel who retaliates against someone who has reported a violation of this Policy in good faith, or who has participated in an investigation of a reported violation, is subject to discipline up to and including termination of employment or contractual arrangement or removal from the Board.

Example: *Community Hospital A, in attempting to negotiate its provider contract with Highmark Health Services has evidence that Highmark Health Services knows the terms and conditions of Community Hospital A's provider contract with other insurers. In the event that Community Hospital A files a complaint against Highmark Health Services, Highmark Health Services may not take any negative action with respect to its relationship with Community Hospital A as a result of this complaint.*

Example: Kathleen works at West Penn Hospital where as part of her duties, she gathers materials to assist the team that negotiates the hospital's rates with insurers. As she is preparing information about the hospital's recent experience providing services to subscribers of National Insurer, she finds an email from her supervisor to an employee of Highmark Health Services attaching West Penn's current agreement with National Insurer. Kathleen reports her findings to the Highmark Chief Privacy Officer, which triggers an investigation and results in serious discipline of her supervisor. Neither the supervisor nor any other System Personnel may take any negative action toward Kathleen for complying with her obligations under this Policy.

XI. No Exceptions

There are no exceptions to this Policy regarding improper access, use or disclosure of CSI.

XII. HIPAA Compliance

Nothing in this Policy is intended to prohibit or otherwise prevent disclosure of information that may include competitively sensitive data elements if the disclosure is necessary, appropriate and required to comply with the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under HITECH, GINA and other modifications to the HIPAA Rules as set forth in 45 CFR Parts 160 and 164

XIII. Amendments

Any amendments to this Policy are subject to approval by the Pennsylvania Insurance Department.

ATTACHMENT A

HIGHMARK

HIGHMARK HEALTH SERVICES COMPANIES

1. Highmark Health Services
    a. United Concordia Companies, Inc.
        i. United Concordia Life and Health Insurance Company
        ii. United Concordia Dental Plans of Pennsylvania, Inc.
    b. HVHC Inc.
        i. VisionWorks, Inc.
        ii. VisionWorks Enterprises, Inc.
        iii. Empire Vision Center, Inc.
    c. Highmark Senior Resources Inc.
    d. Keystone Health Plan West, Inc.
    e. HM Life Insurance Company
    f. HM Health Insurance Company

ALLEGHENY HEALTH NETWORK COMPANIES

1. Allegheny Health Network
    a. HMPG Inc.
        i. Promedix LLC
        ii. Physician Landing Zone PC
            1. Lake Erie Medical Group PC
            2. Premier Medical Associates, PC

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 Specialty Practice Network
    e. West Penn Allegheny Oncology Network
    f. West Penn Physician Practice 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
    b. Erie Regional DMAT PA-3

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.

6. Highmark Health Services
    a. Davis Vision, Inc.
        i. DavisVision IPA, Inc.