Highmark Inc. **Origination Date: September 30, 2013**

Policy Protecting Competitively Sensitive Information **Revision Date: January 23, 2017**

I. Scope

Highmark Inc. 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 Health Policy Protecting Competitively Sensitive Information for the Highmark Health System as defined in that policy and including all companies designated on Attachment A to this Policy as periodically updated. All **Highmark Inc.** 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 Inc. (Highmark) Companies (as buyers of healthcare medical services), Allegheny Health Network (AHN) Companies (as sellers of healthcare medical services), and Highmark Health (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 Companies' knowledge of and ability to influence AHN Companies' negotiations with rival insurers. Similarly, development, implementation and strict compliance with Firewalls is required to restrict AHN Companies' influence on Highmark Companies' negotiations with rival hospitals.

Accordingly, **Highmark Inc.** 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. lD-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

---

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

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 Health*** is the parent entity of both Highmark and AHN.

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

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

F. ***System*** is the collective reference to Highmark Health, Highmark and AHN and any other subsidiary of Highmark Health that receives CSI from Highmark Health, Highmark 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. ***Highmark Inc. 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 respectively and who is directly accountable to the Highmark Health Chief Privacy Officer.

J. ***Senior Privacy Official*** is the **Highmark Inc.** employee responsible for privacy oversight of **Highmark Inc**.

IV. Roles and Responsibilities

A. **Highmark Inc.'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 **Highmark Inc.**
2. Senior Auditor and Compliance Officer, **Highmark Inc.**
3. Senior Legal Officer, **Highmark Inc.**
4. Senior Information Security Officer; **Highmark Inc.**

V. Policy and Administration

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

1. **Highmark Inc.** Personnel who have access to, or are in possession of, any CSI of any Highmark 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. 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 nonaffiliated providers with Sandy because it is CSI.

2. **AHN** Personnel who have access to, or are in possession of, any CSI of any AHN Company shall not disclose such CSI to Highmark or to any Personnel of a Highmark 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. 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 **Highmark Inc.** Personnel must take mandatory CSI Policy training and all newly-hired **Highmark Inc.** Personnel must do so before performing any work. There will be no exceptions to this mandatory requirement. **Highmark Inc.** 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 Health Chief Privacy Officer. At the completion of the mandatory training session and after each refresher training session, all **Highmark Inc.** Personnel shall be required to certify completion of the program and comprehension of the materials presented.

C. All **Highmark Inc.** Personnel must excuse themselves from participation in any activity where their participation would necessarily involve the inappropriate access, use or

disclosure of CSI. Any individual who comes in contact with CSI from either Highmark 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 Health 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 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 **Highmark Inc.** Personnel are encouraged to contact the Highmark Health Chief Privacy Officer or **Highmark Inc.** Director of Privacy or the Senior Privacy Official for **Highmark Inc.** if they have any questions about their responsibilities or other matters pertaining to this Policy.

VI. Infrastructure and Physical Safeguards

A. **Highmark Inc.** 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. **Highmark Inc.** shall continue to use security tools that include electronic interface with the Human Resources systems to provide information regarding the identity of authorized **Highmark Inc.** 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 Health Privacy Department shall work in collaboration with the Chief Information Security Officer to monitor the System, including **Highmark Inc.**, to assure that CSI has not been accessed, used or disclosed in an inappropriate manner.

B. Highmark Health'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. The Internal Audit Department shall conduct regular audits of the System, including **Highmark Inc.**, to ensure compliance with this Policy. Audit findings and observations shall be reported to the Highmark Health Chief Privacy Officer for appropriate remediation and mitigation, and ultimately reported to the Highmark Health Audit Committee, which shall report to the full Highmark Health Board, and to the Audit Committee of the **Highmark Inc.** Board or those performing the audit function, who shall report to the full **Highmark Inc.** Board.

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

D. All **Highmark Inc.** Personnel shall also affirmatively acknowledge that failure to report actual or potential inappropriate access, use or disclosure of CSI may subject the individual to disciplinary action, up to and including termination.

VIII. Violations and Enforcement

A. Inappropriate access, use or disclosure of CSI is subject to corrective action up to and including termination of employment or contractual arrangement, or removal from the Board, consistent with Highmark and **Highmark Inc.** disciplinary procedures.

B. All **Highmark Inc.** Personnel are required to immediately report actual or suspected inappropriate access, use or disclosure of CSI to the **Highmark Inc.** Senior Privacy Official, who shall notify the appropriate Director of Privacy, who shall notify the Highmark Health Chief Privacy Officer. The Highmark Health Chief Privacy Officer, the appropriate Director of Privacy and the **Highmark Inc.** Senior Privacy Official shall

investigate and take appropriate remedial action including determining the cause(s) of any inappropriate access, use or disclosure, mitigating the effects of such access, use or disclosure, 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 Informatics. Glen thanks Helen for the report she generated and sent to him containing Highmark Health 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 AHN Senior Privacy Official.

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

E. Where inappropriate access, use or disclosure of CSI is determined by the Chief Privacy Officer to have occurred, the Chief Privacy Officer is required to report the occurrence to the Department within ten (10) business days of the date the Chief Privacy Officer becomes aware of the occurrence.

Example: Paula is a data analyst supporting the Care Model Redesign initiative at AHN. She has prepared a deck slide containing de-identified discharge summaries for two hundred recent cardiac patients at AHN. The report contains CSI as it includes aggregated reimbursement rates. She sent the report, via secure email to Dana at Highmark Health as Dana is working on a strategic project with the goal of improving outcomes for cardiac patients at AHN. Seconds after Paula sends the email, she notices she sent the email without first checking the recipient field and accidentally sent it to her friend Deana who works for Highmark. Paula immediately calls Deana and alerts her to

the error advising her not to open the email, and to delete it from her inbox. Deana deletes the email before opening it. Paula then calls the technical assistance center (TAC) and the Privacy Department and advises both of them of the mistake. The TAC confirms that the email is no longer in Deana's Outlook file. Because no inappropriate access, use or disclosure of CSI occurred, the matter is not required to be reported to the Department. However, if Deana had opened the email, inappropriate access, use or disclosure of CSI would have occurred and a report to the Department within ten (10) business days after the Chief Privacy Officer became aware of the occurrence would have been required.

IX. Filing a Complaint

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

1. directly to the **Highmark Inc.** Senior Privacy Official or the Highmark Health Chief Privacy Officer,

2. by calling toll-free; 1-877-959-4160,

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

B. The Highmark Health Chief Privacy Officer shall have ultimate responsibility for the administrative enforcement of this Policy. The Highmark Health Chief Privacy Officer, the appropriate Director of Privacy and the **Highmark Inc.** 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

Highmark Inc. is committed to protecting all Personnel, health care providers with whom any Highmark 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, **Highmark Inc.** encourages all Individuals to report good faith concerns about potential inappropriate access, use or disclosure of CSI. 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 **Highmark Inc.** 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 has evidence that Highmark 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, Highmark 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 attaching West Penn's current agreement with National Insurer. Kathleen reports her findings to the Highmark Health 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 inappropriate 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 Department.

ATTACHMENT A

HEALTH CARE INSURERS

1. Highmark Inc.
    a. United Concordia Companies, Inc.
        i. United Concordia Dental Plans of Pennsylvania, Inc.
    b. Highmark Choice Company
    c. HM Life Insurance Company
    d. HM Health Insurance Company
    e. Highmark Senior Health Company
    f. Highmark Coverage Advantage Inc.
    g. Highmark Benefits Group Inc.
    h. HM Centered Health Inc.
    i. Gateway Health Plan, Inc.

HEALTH CARE PROVIDERS

1. Allegheny Health Network
    a. Allegheny Health Network Surgery Center - Bethel Park, LLC
    b. Clinical Services, Inc.
        i. HMPG Inc.
            1. Monroeville ASC LLC*
            2. Physician Partners of Western PA LLC
    c. Grove City Medical Center

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. Premier Medical Associates, PC
        ii. Premier Women's Health
    e. JV Holdco, LLC
    f. Allegheny Clinic Medical Oncology
    g. Peters Township Surgery Center, LLC*
    h. North Shore Endoscopy Center
    i. Allegheny Health Network Home Medical Equipment LLC*

3. Jefferson Regional Medical Center
    a. Prime Medical Group, PCG 1
    b. Primary Care Group 3, Inc.
    c. Primary Care Group 5, Inc.
    d. Primary Care Group 7, Inc.
    e. Primary Care Group 8, Inc.
    f. Primary Care Group 11, Inc.
    g. Family Practice Medical Associates South, Inc.
    h. The Park Cardiothoracic and Vascular Institute
    i. Grandis, Rubin, Shanahan & Associates
    j. Steel Valley Orthopedic and Sports Medicine
    k. Jefferson Hills Surgical Specialists
    l. Pittsburgh Bone, Joint & Spine, Inc.
    m. Pittsburgh Pulmonary and Critical Care Associates
    n. South Pittsburgh Urology Associates
    o. JRMC Specialty Group Practice

4. Saint Vincent Health Center
    a. Regional Heart Network

5. Saint Vincent Health System
    a. Saint Vincent Medical Education & Research Institute, Inc.
    b. Allegheny Health Network Home Infusion LLC*

6. AHN Emerus LLC
    a. AHN Emerus Westmoreland, LLC

7. Endorsed. LLC

*As these entities are member-manager LLCs, they have no boards of directors. Instead, their respective members have adopted the CSI Policy.