Appendices A-L

accompanying

The Pittsburgh Health Information Network (PHIN)

Summary Report

Submitted for the AMA-led

"Effecting Change in Chronic Care: The Tipping Point" AHRQ Grant

by Tania Lyon

Associate Director, Chronic Care

Pittsburgh Regional Healthcare Initiative

Centre City Tower, Suite 2400

650 Smithfield Street

Pittsburgh, PA 15222

(412) 586-6709

(412) 535-0295 [FAX]

tlyon@prhi.org

Contents

Appendices

A: Sample Text of Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is entered into by and between _____, with offices at _____ ("Covered Entity"), and the West Virginia Medical Institute (also d/b/a Quality Insights of Pennsylvania), with offices at 3001 Chesterfield Place, Charleston, WV 25304 ("Business Associate") (Individually a "Party" and collectively the "Parties").

WITNESSETH:

WHEREAS, the Health Insurance Portability and Accountability Act's ("HIPAA") Privacy Regulations impose certain restrictions on the use and disclosure of Protected Health Information ("PHI");

WHEREAS, Covered Entity desires to disclose PHI to Business Associate or allow others to disclose PHI to Business Associate on Covered Entity's behalf and to access PHI from Business Associate to perform certain Treatment and/or Healthcare Operation activities as part of the Initiative; and

WHEREAS, Covered Entity understands that it must enter into this Agreement so that PHI may be disclosed to Business Associate, to allow Business Associate to disclose PHI to Covered Entity and to allow Business Associate to perform and provide services to Covered Entity.

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement to comply with the Privacy Regulations and to protect the interests of both Parties:

I. Definitions

The following terms shall have the meaning ascribed to them in this Section. Other capitalized terms shall have the meaning ascribed to them in the context in which they first appear. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Regulations.

(a) Agreement. "Agreement" refers to this Business Associate Agreement. This Agreement follows and incorporates the Sample Business Associate Contract Provisions found in the Preamble's Appendix to the Final Modification to the Privacy Regulations. *See* 67 Fed. Reg. 53264-66.

(b) Business Associate. "Business Associate" refers to WVMI (also d/b/a Quality Insights of Pennsylvania), located at 3001 Chesterfield Place, Charleston, WV 25304.

(c) Covered Entity. "Covered Entity" refers to _____, with offices located at _____.

(d) Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(e) Initiative. "Initiative" shall refer to the Initiative conceived by working groups of the Pittsburgh Regional Health Initiative ("PRHI") to create a centralized database of medical records and outcomes. The database will be administered and operated by Business Associate, acting on behalf of participating healthcare plans, providers and laboratories. Participating healthcare plans, providers, and laboratories will send PHI to Business Associate, who will be the regional repository for health information. Business Associate will allow participating providers, who obtain consent from patients, to access the database to verify and correct their patients' PHI and use the database as part of their Treatment and/or Healthcare Operation activities. Business Associate will also use PHI to generate condition-specific quality improvement reports that will be disclosed to participating providers.

(f) Privacy Regulations. "Privacy Regulations" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.

(g) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. 164.501, and shall refer to PHI obtained from Covered Entity or obtained by Business Associate on behalf of Covered Entity.

(h) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

(i) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

II. Obligations and Activities of Business Associate

(a) Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required By Law.

(b) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement. To the extent Business Associate obtains PHI in an electronic format, it agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.

(e) Business Associate agrees to ensure that every contractor or agent, to whom Business Associate provides PHI received from Covered Entity or on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to PHI.

(f) Business Associate agrees to provide Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524, access to PHI, in a time and manner reasonably agreed upon by the Parties.

(g) Business Associate agrees to make any amendment(s) to PHI that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, in a time and manner reasonably agreed upon by the Parties.

(h) Business Associate agrees to make its internal practices, books, and records, including any policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary, in a time and manner reasonably agreed upon or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Regulations.

(i) Business Associate agrees to document disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual, in a time and manner reasonably negotiated, PHI given to Business Associate, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

III. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform activities called for by the Initiative. Business Associate may also disclose PHI to healthcare providers participating in the Initiative to assist them with Treatment and/or Healthcare Operation activities.

IV. Specific Use and Disclosure Provisions

(a) Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that such disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the PHI are disclosed that they will remain confidential and used or further disclosed only as Required By Law or for the purpose for which they were disclosed to the

person, and the person notifies Business Associate of any instances of which it is aware that the confidentiality of the PHI have been breached.

(c) Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

(d) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

V. Obligations of Covered Entity

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices, in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

VI. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Regulations if done by Covered Entity, except Business Associate may use or disclose PHI for, and the Agreement provides for, data aggregation or management and administrative activities of Business Associate.

VII. Term and Termination

(a) Term. The Term of this Agreement shall be effective when this Agreement is signed by both parties, and shall terminate when all of the PHI provided by Covered Entity to Business Associate are no longer needed by Business Associate to provide services to Covered Entity and healthcare providers participating in the Initiative.

(b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) Effect of Termination.

(1) Except as provided below in paragraph (2) of this subsection, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity or on behalf of Covered Entity. This provision shall apply to PHI that are in the possession of subcontractors or agents of Business Associate.

(2) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon written notification that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of PHI for so long as Business Associate maintains such PHI.

VIII. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the Privacy or Security Regulations mean the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Regulatory References.

(c) Survival. The respective rights and obligations of Business Associate under Section VII of this Agreement shall survive the termination of this Agreement.

(d) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Regulatory References.

IN WITNESS WHEREOF, Covered Entity and Business Associate have caused this Agreement to be signed and delivered by their duly authorized representatives, as of the date set forth below.

BUSINESS ASSOCIATE

By:_____
Print Name:_____
Title:_____
Date: _____

_____
[Covered Entity]

By:_____
Print Name:_____
Title:_____
Date: _____

B: Legal Opinion on Constituent Liability

June 20, 2003

Via Email

Tania Lyon
Chronic Care Coordinator
Pittsburgh Regional Healthcare Initiative
Centre City Tower, Suite 2150
650 Smithfield Street
Pittsburgh, PA 15222

Re: Covered Entity Liability For Disclosure Of PHI To A Business Associate

Dear Tania:

This letter responds to your request for a summary of the liability issues we discussed during the June 2, 2003, joint committee meeting. Specifically, you ask me to explain certain aspects of liability a covered entity faces when it discloses protected health information ("PHI") to a business associate. The potential liability a covered entity faces can arise from the government as well as third parties, like patients and other covered entities. Each is described in greater detail below.

A. Liability A Covered Entity Faces From Possible Government Action

In terms of liability from possible government action, the concern is that a covered entity discloses PHI to a business associate and then the business associate improperly uses or discloses the PHI or the covered entity fails to adequately monitor its business associate. If this occurs, what is the covered entity's potential liability to the government?

This precise concern was raised and addressed in comments to the final modification to the Privacy Rule. According to the Privacy Rule's comments, "a number of commenters continued to express concern over a covered entity's perceived legality with respect to the actions of its business associate." 67 Fed. Reg. 53252. In response, the Privacy Rule states:

> The Privacy Rule does not require a covered entity to actively monitor the actions of its business associates *nor is the covered entity responsible or liable for the actions of its business associates.* Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the

covered entity take steps to cure the breach or end the violation. See Sec. 164.504(e)(1).

Id (emphasis added).

If a covered entity fails to "take steps to cure the breach or end the violation" of its business associate, then the covered entity may be in non-compliance with the Privacy Rule. Based on the HIPAA statutory language, violations for non-compliance can result in a "penalty of not more than $100 for each violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000." Pub. L. 104-191, Section 1176(a)(1). (Enforcement regulations from HHS are still pending.)

Therefore, a covered entity may be liable to the government for the actions of its business associate only if the covered entity fails to take appropriate action and is found to be in noncompliance. Then, a covered entity's damages may be a much as $100 for each violation.

B. Liability A Covered Entity Faces From Possible Action By Third Parties

Liability faced by a covered entity disclosing PHI to a business associate can come from third parties like patients and other covered entities. For example, if a covered entity discloses PHI to a business associate who improperly uses or disclosures the PHI, then a third party could bring an action against the covered entity for improperly or wrongfully disclosing the PHI to the business associate or failing to monitor the activities of the business associate. Such an action could arise under several legal theories.

First, under most state laws a person suffering damages may bring a tort action for breach of privacy. For example, a patient could bring an action against a covered entity entrusted with its PHI on the grounds that it improperly disclosed PHI to the business associate. Alternatively, the covered entity failed to monitor or take appropriate steps to ensure that the business associate used the PHI properly. In other words, the argument would go that the covered entity violated a patient's expectation of privacy, a protected interest under law.

It is important to note that a breach of privacy action based on the above-described grounds could have been brought even before enactment of HIPAA and the Privacy Rule. A patient could sue a covered entity that improperly discloses PHI to a third party (even with a confidentiality agreement) or failed to adequately monitor its business associate. The issue the court must address, before and after enactment of HIPAA and the Privacy Rule, is whether the disclosure or monitoring was done in accordance with a standard of due care owed to the individual. Before the Privacy Rule it was not clear what standard of due care applies. However, the Privacy Rule now establishes an industry standard of due care.

As explained Part A above, the Privacy Rule sets a very low standard of due care for a covered entity that discloses PHI to a business associate ("where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation"). In terms of monitoring, the Privacy Rule explicitly states that a covered entity does not have to monitor its business associate. If the Privacy Rule is used as the measure of due care, then the standard is quite low. This means a plaintiff would have a difficult time proving that a covered entity disclosing PHI to a business associate failed to comply with a standard of due care if the covered entity does not violate the Privacy Rule. Again, the requirements of the Privacy

Rule for disclosures of PHI to a business associates are minimal. Consequently, the ability of an individual to successfully sue a covered entity that discloses PHI to a business associate is very low.

A second legal theory a third party could use to bring an action against a covered entity that discloses PHI to its business associate arises from consumer fraud laws. A person could argue that a disclosure to a business associate and the improper actions of a business associate violate the representations made by a covered entity in its notice of information practices. According to officials at the Federal Trade Commission ("FTC"), a covered entity's notice of information practices constitutes advertising and potentially subjects the covered entity to consumer fraud. In other words, a patent could bring an action against a covered entity for consumer fraud on the theory that disclosure to a business associate violated the representations continued in the covered entity's notice of information practices. This second theory is yet untested. More importantly, most notices of information practices reference disclosures to business associates.

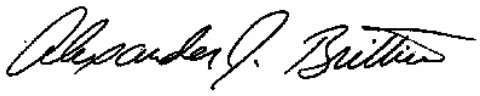
C. Conclusion

As described above, a covered entity may be liable to the government and/or a third party for disclosures of PHI and/or improperly monitoring a business associate. Liability to the government is extremely low; more in the nature of non-compliance. A covered entity's liability to a third party for a breach of privacy rights predates the Privacy Rule. The Privacy Rule, however, helps establish an industry standard of due care owed to an individual by a covered entity when it discloses PHI to a business associate. If a covered entity follows the requirements of the Privacy Rule when disclosing PHI to a business associate, it should not be liable to a third party for the actions of its business associates.

* * *

I hope the forgoing adequately summarizes our earlier discussion about potential liability faced by a covered entity when it discloses PHI to a business associate. If you have any additional questions, please feel free to contact me at your convenience.

Sincerely,



Alexander J. Brittin

cc: John Wiesendanger, CEO, WVMI

C: Legal Opinion on State Law and Mental Health Data

Mental Health Data and State Law Memo

MEMORANDUM

DRAFT

To: **Kim Gray, Privacy Officer, Highmark BC/BS**
From: **Tom Wood, Associate Counsel, Law Dept, Highmark BC/BS**
Lisa Martinelli, Privacy Dept Attorney, Highmark BC/BS
Re: **Pennsylvania statutes governing mental health records**
Date: **July 7, 2003.**

Pennsylvania has two statutes relating to behavioral health that include privacy restrictions more stringent than those found in the HIPAA Privacy Rule:

- The Mental Health Procedures Act, 50 P.S. § 7101; and
- The Drug and Alcohol Abuse Control Act, 71 P.S. § 1690.101 et seq.

Under these statutes, most disclosures for purposes other than treatment will require patient consent, and there is no general permission to re-disclose patient information for "treatment, payment or health care operations" as is found in the HIPAA regulations.

A. Mental Illness

1. Treatment

The restrictions in the Mental Health Procedures Act are limited to persons "in treatment." The initiation of "treatment" requires that individuals submit (either voluntarily or involuntarily) to a medical evaluation, and that the evaluation result in specific finding of a need for treatment and a recommended treatment plan. In the absence of a formal evaluation and finding of a need for specific "treatment," as defined in the statute, the confidentiality provisions would probably not supersede the HIPAA privacy regulations. Routine screening and treatment for depression among patients who are not currently undergoing "treatment" would probably be governed by the HIPAA privacy standards.

Regulations adopted under the Mental Health Procedures Act establish a formal process for initiating treatment of mental illness. The process must be initiated by an application, made on an official form, either voluntarily (under 55 Pa. Code § 5100.72) or involuntarily (under 55 Pa. Code § 5100.86). Once treatment is initiated by one of these methods, the regulations require a formalized process of review, and discharge, either at the expiration of any court-ordered period of involuntary treatment (55 Pa. Code §§ 5100.87, 5100.88), or when the patient is found to no longer require treatment (55 Pa. Code § 5100.77). We understand that, in practice, discharge orders are definitive, and clearly indicate that treatment under the Mental Health Procedures Act has terminated. It should therefore be possible to identify with some precision those persons to whom the stricter confidentiality provisions of the Act apply. Health records pertaining to the period between admission and

discharge would be subject to the stricter standard; those pertaining to subsequent outpatient treatment would be subject to the HIPAA rules.

2. Confidentiality and Written Consent

As discussed above, most data used in the PRHI initiative will probably be governed by standard HIPAA privacy rules. However, if the initiative uses any data relating to treatment under the Mental Health Procedures Act, the rules for use of data differ somewhat from the HIPAA rules. The Pennsylvania mental health regulations contain specific rules governing disclosure of treatment records. Nonconsensual disclosures are permitted under 55 Pa. Code § 5100.32, attached as Exhibit "A." Nonconsensual disclosures are limited to those actively engaged in treating the individual; to third party payors (limited to staff names, the dates, types and costs of therapies or services and a short description of the general purpose of each treatment session or service); to those participating in utilization review; and in response to a court order. In all situations that not specifically listed as nonconsensual releases, the patient's written consent is required. Section 5100.34 of the regulations, attached as Exhibit "B," prescribes the content of a valid consent document, and provides that all disclosures of treatment information covered by the Act be accompanied by a written statement that reads: *This information has been disclosed to you from records whose confidentiality is protected by State statute. State regulations limit your right to make any further disclosure of this information without prior written consent of the person to whom it applies.*

Subject to the disclosure statement quoted above, the regulation seems to allow for free exchange of information among providers involved in the individual's treatment, and to payors for purposes of claim payment.

B. Drug and Alcohol Abuse

The confidentiality provisions of the Drug and Alcohol Abuse Control Act are stricter than those pertaining to general mental illness. The statute requires consent for all disclosures, and even with consent, disclosures are limited to (1) medical personnel exclusively for purposes of treatment and (2) "government or other officials exclusively for the purpose of obtaining benefits due the patient." Unlike the Mental Health Procedures Act, this statute appears to cover all records of substance abuse patients, even after they have left the formal treatment setting. Section 8 of the act (71 P.S. § 1690.108) extends the confidentiality provisions to *"all patient records and all information contained therein relating to drug or alcohol abuse or drug or alcohol dependence prepared or obtained by a private practitioner, hospital, clinic, drug rehabilitation or drug treatment center…"*

Procedural rules for the initiation of inpatient drug and alcohol abuse treatment are found at 28 Pa. Code, Part V. The regulations are quite specific as to what constitutes "treatment." See 28 Pa. Code, Part V, Chapter 709. However, since the act does not distinguish clearly between records of persons "in treatment," and records held by primary care physicians or other providers, disclosure of any diagnosis or procedure code relating to substance abuse, even for patients not in a formal treatment program, will probably require a written consent.

The above discussion is based on a review of Pennsylvania law only, and does not address the disclosure or consent requirements of any other states.

EXHIBIT A
PENNSYLVANIA ADMINISTRATIVE CODE
TITLE 55. PUBLIC WELFARE
PART VII. MENTAL HEALTH MANUAL
SUBPART C. ADMINISTRATION AND FISCAL MANAGEMENT
CHAPTER 5100. MENTAL HEALTH PROCEDURES
CONFIDENTIALITY OF MENTAL HEALTH RECORDS
Current through Supp. 342 (May 2003)

§ 5100.32. Nonconsensual release of information.

(a) Records concerning persons receiving or having received treatment shall be kept confidential and shall not be released nor their content disclosed without the consent of a person given under § 5100.34 (relating to consensual release to third parties), except that relevant portions or summaries may be released or copied as follows:

(1) To those actively engaged in treating the individual, or to persons at other facilities, including professional treatment staff of State Correctional Institutions and county prisons, when the person is being referred to that facility and a summary or portion of the record is necessary to provide for continuity of proper care and treatment.

(2) To third party payors, both those operated and financed in whole or in part by any governmental agency and their agents or intermediaries, or those who are identified as payor or copayor for services and who require information to verify that services were actually provided. Information to be released without consent or court order under this subsection is limited to the staff names, the dates, types and costs of therapies or services, and a short description of the general purpose of each treatment session or service.

(3) To reviewers and inspectors, including the Joint Commission on the Accreditation of Hospitals (JCAH) and Commonwealth licensure or certification, when necessary to obtain certification as an eligible provider of services.

(4) To those participating in PSRO or Utilization Reviews.

(5) To the administrator, under his duties under applicable statutes and regulations.

(6) To a court or mental health review officer, in the course of legal proceedings authorized by the act or this chapter.

(7) In response to a court order, when production of the documents is ordered by a court under § 5100.35(b) (relating to release to courts).

(8) To appropriate Departmental personnel § 5100.38 (relating to child or patient abuse).

(9) In response to an emergency medical situation when release of information is necessary to prevent serious risk of bodily harm or death. Only specific information pertinent to the relief of the emergency may be released on a nonconsensual basis.

(10) To parents or guardians and others when necessary to obtain consent to medical treatment.

(11) To attorneys assigned to represent the subject of a commitment hearing.

(b) Current patients or clients or the parents of patients under the age of 14 shall be notified of the specific conditions under which information may be released without their consent.

(c) Information made available under this section shall be limited to that information relevant and necessary to the purpose for which the information is sought. The information may not, without the patient's consent, be released to additional persons or entities, or used for additional purposes. Requests for information and the action taken should be recorded in the patient's records.

EXHIBIT B

PENNSYLVANIA ADMINISTRATIVE CODE
TITLE 55. PUBLIC WELFARE
PART VII. MENTAL HEALTH MANUAL
SUBPART C. ADMINISTRATION AND FISCAL MANAGEMENT
CHAPTER 5100. MENTAL HEALTH PROCEDURES
CONFIDENTIALITY OF MENTAL HEALTH RECORDS
Current through Supp. 343 (June 2003)

§ 5100.34. Consensual release to third parties.

(a) Access to records, as defined in § 5100.33(b) (relating to patient's access to records and control over release of records) will be granted to persons other than the patient upon written consent of the client/patient. With the consent, copies of excerpts or a summary of a record may be provided to specific persons at the discretion of the director. If copies of excerpts or summaries are provided, a charge may be made against the patient or person receiving the record for the cost of making the copies. The facility may require payment for the copies in advance.

(b) When a patient designates a third party as either a payor or copayor for mental health services, this designation carries with it his consent to release information to representatives of that payor which is necessary to establish reimbursement eligibility. Unless otherwise consented to by the patient, information released to the third-party payors shall be limited to that necessary to establish the claims for which reimbursement is sought.

(c) Clients, patients, or other persons consenting to release of records are to be informed of their right, subject to § 5100.33 to inspect material to be released.

(d) When records are released or disclosed under § 5100.32 (relating to nonconsenual release of information) or subsections (a) and (b) the written or oral disclosure shall be accompanied by a written statement which reads as follows: "This information has been disclosed to you from records whose confidentiality is protected by State statute. State regulations limit your right to make any further disclosure of this information without prior written consent of the person to whom it pertains."

(e) The limitation in subsection (d) does not prohibit the re-release of information in accordance with § 5100.32.

(f) Each facility shall prepare a form for use in the voluntary release of records which shall meet the following requirements:

(1) A time limit on its validity which shows starting and ending dates.

(2) Identification of the agency or person to whom the records are to be released.

(3) A statement of the specific purposes for which the released records are to be used.

(4) A statement identifying the specific relevant and timely information to be released.

(5) A place for the signature of the client/patient or parent or guardian and the date, following a statement that the person understands the nature of his release.

(6) A place for the signature of a staff person obtaining the consent of the client/patient or parent or guardian and the date.

(7) A place to record a verbal consent to release of information given by a person physically unable to provide a signature and a place for the signatures of two responsible persons who witnessed that the person understood the nature of the release and freely gave his verbal consent.

(8) Indication that the consent is revocable at the written request of the person giving consent, or oral request as in paragraph (7).

(g) A mental health facility receiving a request for information from a governmental agency may accept that agency's release of information form if signed by the patient/client or the person legally responsible for the control of information unless the patient has specifically expressed opposition to that agency receiving information.

D: Legal Opinion on Need for Patient Authorization

Patient Authorization Memo

Draft

Memorandum

TO: Kim Gray

FROM: Kirk J. Nahra

DATE: July 7, 2003

RE: Highmark Information-Sharing with Physicians for Care Coordination

---

You have asked me to review the HIPAA privacy implications of the following situation.

Factual Background

Highmark is involved in discussions with other entities in the health care industry, related to efforts to improve the quality of medical care provided to patients/members. For that purpose, Highmark (along with other health care entities) has retained a vendor who will, pursuant to a business associate contract with Highmark, receive certain data from Highmark and then, pursuant to Highmark's instructions, distribute this information (considered PHI under HIPAA) to physicians. The purpose of this information distribution is to provide physicians with data on Highmark members, with Highmark's goal for disclosure of PHI being to improve the quality of care provided to its members. The current model relates to information being provided to primary care physicians about health care treatments provided by other physicians to Highmark members. Highmark's goal in sharing this information is to allow the PCPs to better coordinate care for the Highmark members.

In addition to Highmark's participation, other health care providers also will be providing PHI to the same vendor, as a business associate of each participating health care provider. The vendor, acting pursuant to business associate arrangements with all of the participants

that are sharing information, will prepare patient-specific reports that are available to health care providers, containing consolidated treatment information about their own patients.

Legal Analysis

The Privacy Rule allows PHI to be used and disclosed or treatment, payment and health care operations purposes, without the need for any explicit permission from an individual patient. A covered entity also may disclose PHI to another covered entity for treatment activities of a health care provider. In addition, a covered entity may disclose PHI to another covered entity for certain health care operations of the entity that receives the PHI if each entity has or had a relationship with the individual (the "certain" health care operations include the purposes identified below – i.e., care coordination). *See* 45 C.F.R. § 164.506(C)(4). Accordingly, if a use or disclosure fits these "TPO" purposes, the Privacy Rule does not require Highmark to obtain a member/patient authorization. Moreover, the Privacy Rule does not impose any specific limitations on the recipients of PHI when a covered entity discloses PHI for its health care operations.

It is my view that the care coordination activities described above all will fit within TPO – and therefore the Privacy Rule will not require authorizations from patients. There are a variety of ways in which this information-sharing fits within the TPO categories. First, from Highmark's perspective, all of the PHI is being disclosed (by Highmark's business associate/vendor on Highmark's behalf) for purposes that fit within the definition of "health care operations." This definition allows the use and disclosure of PHI for "conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;" Highmark's purpose in disclosing PHI is to improve the quality of care provided to Highmark members and to allow for better coordination of care for Highmark members. Therefore, the disclosure is permitted under the Privacy Rule without authorization.

Second, the purpose of the data-sharing program you have identified is to coordinate care of Highmark members, as part of an overall quality assurance program. The program is designed to ensure that member's health is "coordinated" through disclosure of appropriate information to Primary Care Physicians. Accordingly, in connection with its care coordination and quality assurance programs, Highmark (or other health plans) is permitted to "disclose" PHI in connection with these activities. Obviously, this disclosure is subject to the minimum necessary requirements (which would presumably preclude, for example, disclosure of PHI to all physicians in a community, on the off-chance that a patient might go to on of those physicians). There is no requirement under the Privacy Rule that disclosures for Highmark's health care operations be to any particular kind of entity (in fact, the restriction on disclosures of PHI where both covered entities have a relationship with the member only applies where one covered entity (e.g., Highmark) is asked to disclose PHI for the other covered entity's health care operations). So, if Highmark were requested to disclose PHI to a doctor solely for the doctor's health care operations, the requirements of § 506(c)(4) would need to be met (which probably could be met in this situation). Here, however, where the disclosure is for Highmark's health care operations, the Privacy Rule does not impose the § 506(c)(4) requirements. In addition, the fact that a doctor that receives this information may in turn use the PHI for treatment purposes does not change the initial allowability of the disclosure. Once the doctor "has" the PHI, he, in turn, can "use or disclose" the PHI for treatment purposes. The data-sharing program, designed as it is to focus disclosure of PHI to PCPs (whose responsibility is to effectively manage care of their individual patients), fits within these health care operations categories. Under this portion of the Rule, therefore, (and subject to any additional state law limitations), this PHI can be disclosed in this context without the need for any patient authorization.

Third, to the extent that health care providers are disclosing PHI to the same business associate, with the expectation that this information will be disclosed to other health care providers that are treating the same patient, this disclosure also fits within the Privacy Rule. The disclosure by each physician is for that health care provider's health care operations, for the same rationale as described above for Highmark. In addition, even if the separate requirements of 506(c)(4) are involved, this disclosure can be justified because it is a disclosure by one covered entity health care provider for quality improvement and care

coordination purposes, and PHI is only shared between health care providers that both have a relationship with an individual patient.

More directly, to the extent that disclosures of PHI are between health care providers, these disclosures also can be justified as part of each health care provider's treatment of the patient. Under the Privacy Rule, "treatment" means "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another." Beyond the "health care operations" component, these disclosures are being made so that overall treatment of the patient can be improved, primarily so that medical treatments are consistent and not in conflict with one another, and therefore health care provider to health care provider disclosures, even where a mutual business associate is "in the middle," are allowed under the Privacy Rule.

Accordingly, all of the relevant disclosures of PHI as part of this overall project can be justified under the Privacy Rule as part of TPO, and therefore authorizations from individual patients would not be needed.[1]

Additional Information

In evaluating the overall issues related to this project, it also is worth considering the recent announcement of HHS related to development of an electronic medical record. In a July 1, 2003 press release, HHS Secretary Thompson announced "new steps" in building a "national electronic health care system that will allow patients and their doctors to access their complete medical records anytime and anywhere they are needed, leading to reduced medical errors, improved patient care, and reduced health care costs." This announcement, again according to the press release, is "part of the ongoing HHS effort to develop the National Health Information Infrastructure by encouraging and facilitating the widespread use of modern information technology to improve the nation's health care system."

[1] I have not reviewed the possibility of establishing an "organized health care arrangement," as the administrative details of this approach are quite substantial. If these administrative difficulties can be overcome and you would like to pursue this option, please let me know so that I can review the HIPAA implications of this approach.

According to Secretary Thompson, "[b]anks and other financial institutions all across the country can talk to each other electronically, which has streamlined customer transactions and reduced errors. . . . We want to do the same thing for the American health care system. We want to build a standardized platform on which physicians' offices, insurance companies, hospitals and others can all communicate electronically, which will improve patient care while reducing the medical errors and the high costs plaguing our health care system." According to Secretary Thompson, "[t]his system will prove invaluable in facilitating the automated exchange of clinical information needed to protect patient safety, detect emerging public health threats, better coordinate patient care and compile research data for patients participating in clinical trials."

While the details of this program obviously remain to be worked out, this effort to develop a much more broad-based system for distribution of health care information seems to indicate that the type of program envisioned by Highmark is not only consistent with HIPAA, but is the kind of goal that HHS seems to be actively encouraging.

Conclusion

Accordingly, my view is that there is ample support under the Privacy Rule for the disclosure of PHI for the health care operations and treatment purposes outlined in this memorandum. There is no need, therefore, under the Privacy Rule to obtain patient authorization for these disclosures.

This opinion focuses solely on the allowability of these disclosures under HIPAA. It does not address any issues under Pennsylvania (or other state) law. It also does not address in any way the "desirability" of these disclosures. As with many aspects of the HIPAA rule, the mere fact that a disclosure is "allowed" does not mean that it should be made, or that patients will not complain even about a legally appropriate disclosure. I leave those discussions for the remainder of the group.

Please let me know if you have any questions or comments on this analysis, or if you would like any additional information.

E: Memo Regarding Background on CMS and the PHIN

MEMO

TO: PRHI Leadership

FROM: Tania Lyon

DATE: June 11, 2004

RE: Background on CMS and the PHIN:
History, Current Assessment, and Next Steps

The GOALs of this research were to
(1) review our past interactions with CMS around the PHIN,
(2) determine current CMS regulations on and precedents for the sharing of patient-identified Medicare data, and
(3) determine the best possible contact for Paul O'Neill to pursue further action with CMS

Two Possible Approaches for gaining CMS support for the PHIN

1) As a special project under WVMI's QIO contract
2) As a research or demonstration project

(1) Last spring WVMI approached CMS about setting up the PHIN under its QIO contract.

- They first met with Dennis Stricker (Head of the CMS IT division) and his assistant Will Mados. Stricker informed them that there was a draft policy forthcoming that WVMI would need to adhere to in such a project. This policy was released July 10, 2003 from Stricker and Steve Jencks with the following language:

  > "QIOs may not develop tools that transmit privacy data without CMS approval. In order for a QIO to develop a tool with the intention of transmitting privacy data, the QIO must submit a concept proposal to the Special Study Review Panel (SSRP)."

  WVMI proceeded by submitting a concept paper for the PHIN to the SSRP as required. It was crafted to show how the PHIN coincides with QIO mandates and how it could meet security requirements.

- This concept paper was denied by Bill Rollow (Head of the QIO division). In a follow-up meeting with Bill Rollow and Will Mados, WVMI was told that CMS was not interested in pursuing data sharing projects that did not include data from physician offices—part of a growing movement to push EMRs into every outpatient setting. (The PHIN works only with claims data and lab values). At this point, WVMI discontinued their efforts to gain approval for the PHIN as a QIO special project.

- At the same time, Ken Segel approached Steve Jencks directly for support in a letter describing the PHIN project, but also received a negative response.

- In May 2004, Bill Rollow and Dennis Stricker released a policy memo to all QIOs "to clarify the management and control of data contained in the data warehouse, as well as the rules governing the use of this data."

    - The language in this memo is somewhat ambiguous and can be alternately read to be in favor or against a structure like the PHIN.

      For example:

      "…regulations…require that a QIO provide information on a patient to the patient…at his or her request, as long as all other patient and practitioner identifiers have been removed."

      Analysis: Could a patient granting permission to a physician to pull data from the PHIN fit into these parameters? Page: 22
      The memo does not appear to contemplate QIOs releasing information to a third party, but nor does it explicitly forbid it.

      "…QIOs would be able to release information… back to a provider or practitioner that contains patient, practitioner or institution-specific data that was originally furnished by them to the QIO…This info can be viewed as quality-related information necessary to assist providers and practitioners in their quality improvement activities, and therefore can be released back to the provider or practitioner for quality improvement purposes."

      Analysis: Couldn't PHIN data be considered as originally furnished by the practitioner and drawn on for quality improvement purposes? On the other hand this doesn't seem to include pulling down data from other physicians who also treat the same patient, as these would be used for treatment purposes rather than quality improvement--see below:

      "…any information the QIO releases cannot contain claims data from any other practitioner or provider who has furnished treatment to the same patient."

      Analysis: A critical omission here is that there is no provision for individual patient consent to over-ride this directive.

- Most recently, CMS released a one-page "Proposed Policy" on June 8, 2004 with the following opening paragraph:

  > "Effective immediately, QIOs are not allowed under the core contract to develop new registry systems or to enhance…existing QIO-developed registry systems."

  This could represent a deliberate move to block QIO involvement in centralized registry efforts like the PHIN; the draft policy appears to be shepherding all QIOs toward a very specific direction—namely supporting the adoption of on-site EMRs with specified functions in all Medicare-related practices.

(2) One response to these restrictive program directives is to abandon a QIO-based approach to CMS for the PHIN and pursue the option of a research/demo project—one of the only areas that permits the release of patient-identified Medicare data.

Conversations with Linda Magno (who oversees demo project development) and Spike Duzor (Chair of the CMS Privacy Board) have yielded the following.

CMS would be likely to approve the release of patient-identified data under the following circumstances:

- If the research project is something that CMS wants an answer to and would research itself if it had the resources
- If CMS believes that the research would benefit Medicare patients or improve the Medicare program
- However, physicians have successfully lobbied for the same level of privacy as patients which may complicate our efforts to share multiple physician data based on patient consent (as opposed to physician consent).

If we do successfully get established as a CMS demo project, then CMS would likely make WVMI (as the data holder) its agent. It was implied, however, that Medicare beneficiaries would have to be informed of the demo and the release of their data, which is probably a requirement we could work with (informing is much easier than requiring individual consent).

Spike Duzor indicated to me that this kind of chronic disease management project (i.e. the PHIN) had already been demonstrated and that our proposal may not represent new research. In fact, CMS has recently launched several disease management demo projects and is about to start another one involving 30,000 enrollees around the country.

Duzor told me that when all these demos are complete and effective processes are proven, then they will become standard Medicare benefits to be mandated (and funded) by Congress. He seemed to imply that CMS was more interested in research than in supporting actual quality improvement projects that have emerged outside of CMS. *I have yet to discover a single precedent for CMS to cooperate with existing quality improvement efforts in releasing Medicare data.*

He did however clarify that what we are asking for is a POLICY CALL, not a legal or technical issue. He suggested we contact the following:

David Kreiss Special Asst to the Administrator and a specialist in disease management at CMS.

How should we proceed based on this information?

F: Individual Patient Report (Diabetes)

Diabetes Mellitus PHIN Patient Profile

NAME:	SEX:	DOB:
Health Plan:	Claim #:	

Outpatient Care

Last 5 Practitioner Visits

DATE	PRACTITIONER NAME	CPT CODE OF VISIT	Days elapsed between visits

Last Eye Exam Claims

DATE	PRACTITIONER NAME	CPT CODE	Report Received?	Was exam dilated retinal?	Days elapsed since last exam
			Y / N	Y / N	
			Y / N	Y / N	

Other Preventive Measures to assess and track (data not available from PHIN)

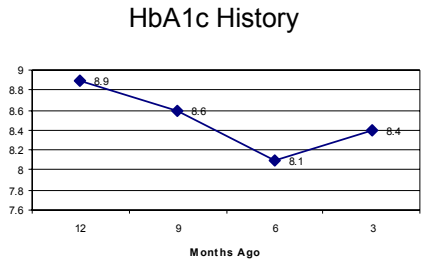
Weight	Smoking (Counseling and/or Pharmacological Intervention)
Blood Pressure	Aspirin Use in patients >40 years old
Foot Exam with every visit	Creatinine Level, annual
Influenza Vaccination, annual	Review of Self-management Plan with every visit (includes assessment of medical nutrition, exercise, etc.)
Pneumococcal Vaccine, once at diagnosis, once >65 yrs old*	

* Or five years after initial vaccination

Laboratory Results

Hemoglobin A1c (%)

DATE	RESULT	LAB	LAB SPECS



Lipid Profile

DATE	CHOLESTEROL			Triglycerides	Fasting (Y/N)	LAB
	Total	LDL	HDL			

Microalbumin ☐ Not indicated			
DATE	TYPE OF TEST	RESULT	LAB

Medications

Diabetes-related Drugs (prescriptions filled in last ___ months) sorted by ☐ date dispensed, ☐ NDC code

DATE DISPENSED	DRUG	DOSAGE	DAYS SUPPLY	# TIMES REFILLED	PRESCRIBING PHYSICIAN

Other Medications (prescriptions filled in last ___ months) sorted by ☐ date dispensed, ☐ NDC code

DATE DISPENSED	DRUG	DOSAGE	DAYS SUPPLY	# TIMES REFILLED	PRESCRIBING PHYSICIAN

G: Individual Patient Report (Depression)

Major Depressive Disorder PHIN Patient Profile

NAME:	SEX:	DOB:
Health Plan:	Provider #:	

Outpatient Care

Initial Diagnosis for Depression (see next page for recommended diagnostic criteria)

DATE	PRACTITIONER NAME	BASED ON DATE
		☐ of first ICD9 depression code ☐ of first antidepressant drug claim ☐ reported to PHIN by diagnosing physician

Last 5 Practitioner Visits *(The NCQA-HEDIS Guidelines recommend at least 3 follow-up visits within 12 weeks of starting care for depression)*

DATE	PRACTITIONER NAME	CPT CODE OF VISIT	Days elapsed since initial diagnosis

Other Measures to assess and track (data not available from PHIN)

Overall Assessment of Symptoms* ☐ worse, ☐ same, ☐ improved, ☐ in remission**	Suicide Risk Assessed: (Y / N) Side Effects Related to Medication: assessed (Y / N)
Adherence to Treatment ☐ good ☐ fair ☐ poor	Classification of MDD Severity ☐ mild ☐moderate ☐severe
Psychotherapy: indicated (Y / N), prescribed (Y / N), continued (Y / N)	Referral for Psychiatric Consultation: indicated (Y / N), referred (Y / N)

Medications:

(Depressive symptoms commonly continue due to lack of adherence to treatment or under-treatment. See new patients at 2-4 weeks and twice more in the initial 12 weeks to reassess adequacy of patient response to medication.)

Antidepressant Drugs (prescriptions filled in last ___ months) sorted by ☐ date dispensed, ☐ NDC code

DATE DISPENSED	DRUG	DOSAGE	DAYS SUPPLY	# TIMES REFILLED	PRESCRIBING PHYSICIAN

Other Medications (prescriptions filled in last ___ months) sorted by ☐ date dispensed, ☐ NDC code

DATE DISPENSED	DRUG	DOSAGE	DAYS SUPPLY	# TIMES REFILLED	PRESCRIBING PHYSICIAN

* A commonly used assessment tool, the PHQ-9, is available at <http://www.americangeriatrics.org/education/dep_tool_05.pdf>
** The APA guidelines recommend continuing effective treatment a minimum of 16-20 weeks following remission of symptoms to prevent relapse. If treatment is discontinued, patients should be carefully monitored for relapse, and treatment should be promptly reinstituted if relapse occurs.

Diagnostic Criteria

At least 5 of the following symptoms during the same two week period (must include symptom 1 *or* 2)

1. Depressed Mood Y or N	2. Marked diminished interest/pleasure Y or N	3. Significant weight loss or gain Y or N
4. Insomnia or hypersomnia Y or N	5. Psychomotor agitation/retardation Y or N	6. Fatigue or loss of energy Y or N
7. Feelings of Worthlessness Y or N	8. Diminished ability to concentrate Y or N	9. Recurrent suicidal ideation Y or N

Major Depressive Disorder diagnosis confirmed? Y or N*

* Treatment may be indicated in the absence of a confirmed diagnosis of MDD

H: Short Term PHIN Evaluation Criteria

Evaluation Criteria for Pilot Phase of the PHIN:
Draft 2-23-04

Please send comments and suggestions for editing these criteria to Tania Lyon <tlyon@prhi.org>

1) FUNCTIONALITY: How well does it work? Does it work as intended?
Evaluated by WVMI/QIO staff processing the data

- Timeliness
  What % and what kind of data is available within 1 month? 2 months? 3 months? Longer?

- Accuracy of identifying algorithms
  (# of corrections sent back from practice/# patients sent to practice from PHIN = PHIN algorithm accuracy level)

- Accuracy of Master Patient Index (% ambiguities requiring human intervention)

- Accuracy of Claims Data itself (# of errors reported by practices)

- Response Time for the website to generate requested reports

2) OPERATIONAL FIT
Evaluated by queries to users, site visits, etc.

- Is the practice training/education on how to use the PHIN effective?

- Are you able to use the PHIN without undue time burdens on your staff?

- How is the PHIN used in your practice? How does it fit into the existing flow of operations? How much have you had to change in order to use the PHIN?

- How could the PHIN be designed differently to fit better with your office operations?

3) USER SATISFACTION: How well do users perceive that it works?
Evaluated by questionnaires, listserv discussions, or interviews with users

- Is this system useful to you?
- Did the PHIN meet your expectations?
- How can physician expectations be better aligned with what PHIN can and cannot offer?
- Would you recommend it to your colleagues?
- Would you lobby other data providers (labs and health plans) to enroll?
- Will you continue to use it after the pilot?
- What feedback, positive or negative, have you encountered from patients when you discuss the PHIN with them?

4) LEVEL OF ENGAGEMENT/USAGE: To what extent are users putting it to work?
Evaluated by WVMI/QIO staff handling data

- How much feedback do users provide to clean up their registry lists?
- How often do users call up each kind of report?
- After 3 months of using the PHIN (once initial registry has been cleaned and new sets of data are coming in on patients) are practices pulling reports on the patients the PHIN has activity for? In other words, are practices pulling reports on patients who we know are claiming office visits with them?
- What % of patients in a practice **opt in** to share diabetes data? Depression data?
- What % actively **opt out**?
- What are some reasons given for opting out? *Voluntary mailer postcards could be provided in practice offices for concerned patients to provide feedback:*

  - ☐ Don't trust technical security of database
  - ☐ Don't trust certain doctors with data from other doctors
  - ☐ My doctors already have access to the data they need to treat me effectively
  - ☐ Other: _____

I: Long Term PHIN Evaluation Criteria

Evaluation Criteria for Long-term Regional Impact of the PHIN:
Draft 2-23-04

Please send comments and suggestions for editing these criteria to Tania Lyon <tlyon@prhi.org>

1) CLINICAL MEASURES ON REGIONAL LEVEL

- Changes in adherence rates to AMA/Consortium performance measures or HEDIS standards among PHIN users (= changes in numbers of patients getting minimum standard of care)
- Measures of changes in HEDIS adherence rates and lab test results among PHIN users compared to overall regional data from PHC4?
- Change in hospitalization rates for diabetes- or depression-related causes

2) PENETRATION LEVELS

- What % of physician practices in the region has enrolled to use the PHIN?
- What are the usage rates of enrolled users (i.e. what % of users actually draw reports from the PHIN and, of those, to what extent are they pulling reports on patients with office visit claims linked to their practices)?
- What % of patients opt in? opt out?

3) COST-BENEFIT ANALYSIS

- How have actual costs compared to projected cost of 3-year launch period?
- Have participating practices experienced an increase or decrease in costs associated with using the PHIN?
- Have health plans experienced a reduction in acute-care claims charges among patients monitored via the PHIN?
- Have participating laboratories experienced an increase in diabetes-related testing linked to PHIN usage?
- How do estimated regional PHIN-related savings compare to regional PHIN costs?

J: Proposed 3-Year Budget for PHIN

Proposed 3 Year Budget
for the Pittsburgh Health Information Network (PHIN)

	Year 1		Year 2	Year 3
	Months 1-6	Months 7-12		
ONE-TIME START-UP COSTS				
Dedicated Server	$11,000			
Database Server	$11,000			
Oracle DBMS – unlimited license	$30,000			
Router, firewall	$8,000			
Digital Certificate		$5,000		
Intrusion Detection		$125,000*	** = required technology by CMS for Medicare data*	
Tape backup		$15,000		
Rack Mount		$4,000		
UPS	$2,000			
Microsoft License	$2,000	$35,000		
Interface with each data provider (need for interfaces yet to be determined) $10,000 each; 3 plans and 5 labs for pilot; 6 plans and 32 labs for full implementation in year 2		$80,000	$300,000	
TOTAL:	**65,800**	**$264,000**	**$300,000**	
CONTINUING COSTS: LABOR (includes benefits) AND MAINTENANCE				
Physician Practice Training ($100-200 each; 12 practices in pilot; estimated 100 practices each year thereafter)	$1,800	$7,500	$15,000	$15,000
Database Management at WVMI				
Project Director		$50,000	$100,000	
Programmer	$32,500	$32,500	$65,000	$32,500
Network Administrator	$7,000	$7,000	$14,000	$14,000
Data Quality Specialist	$4,000	$4,000	$8,000	$8,000
Administrative Staff	$4,000	$4,000	$8,000	$8,000
Tape Purchase Library	$1,000	$1,000	$1,000	$1,000
TI communications line	$10,800	$10,800	$21,600	$21,600
TOTAL:	**$59,300**	**$116,800**	**$532,600**	**$100,100**
GRAND TOTAL:	**$125,100**	**$380,800**	**$532,600**	**$100,100**

3 Year Grand Total = $1,138,600

K: Technical Feasibility Pilot Budget

Proposed Demonstration Pilot Budget
for the Pittsburgh Health Information Network (PHIN)
[projected as of 6-3-04]

	Months 1-4
ONE-TIME START-UP COSTS	
Dedicated Server	$11,000
Database Server	
Oracle DBMS – unlimited license	
Router, firewall	$4,000
Digital Certificate	
Intrusion Detection	
Tape backup	
Rack Mount	
UPS	
Microsoft License	$1,000
Physician Practice Training ($100-200 each; 8 practices in pilot)	$1,200
TOTAL:	**$17,200**
CONTINUING COSTS: LABOR (includes benefits) AND MAINTENANCE	
Database Management at WVMI	
Project Director	
Programmer	$10,800
Network Administrator	$1,000
Data Quality Specialist	$1,000
Administrative Staff	$1,000
Tape Purchase Library	
TI communications line	$5,400
TOTAL:	**$19,200**
GRAND TOTAL:	**$36,400**

L: Press Release on the Pennsylvania e-Health Technology Consortium

Contacts:
Chuck Moran, Pennsylvania Medical Society, (717) 558-7820
Krista Davis, Quality Insights of Pennsylvania, (877) 346-6180, ext. 7617

For release on March 15, 2005

Pennsylvania begins big step forward on electronic health records, patient safety

Consortium starts work on e-health infrastructure to be tied into national efforts

(Harrisburg, Pa.) A consortium of 28 health care organizations plan to build the Pennsylvania electronic patient data network that will be tied into a national system so that patients and their doctors can securely access medical records from any part of the country.

Informally called the Pennsylvania e-Health Technology Consortium, the group says efforts to build and standardize a secure national electronic medical record network will improve patient safety, save on health care spending, and help doctors treat patients faster.

Founded by Quality Insights of Pennsylvania and the Pennsylvania Medical Society, the consortium was sparked by President Bush's call for the health care community to switch from paper to electronic health records within 10 years.

"This consortium will play a major role in the development of Pennsylvania's infrastructure that eventually will move the state light years ahead into the future of health care," said Donald F. Wilson, M.D., medical director of Quality Insights of Pennsylvania based in Wayne, Pa. "This project will be part of a larger effort that will change the way medicine is practiced throughout the country."

As a quality improvement organization, Quality Insights of Pennsylvania has been charged by the Center for Medicaid and Medicare Services to foster the Pennsylvania-based electronic networks, also known as Regional Health Information Organizations.

Others agree with Dr. Wilson, and add that the consortium will help patients and their doctors work together.

"Imagine a person from Central Pennsylvania visiting a relative in New Mexico," said William W. Lander, M.D., president of the Pennsylvania Medical Society in Harrisburg. "That person for some reason gets violently sick and is rushed to the local emergency room. Once this network is built, that individual's health records essentially travel with him. Emergency medicine physicians at the hospital in New Mexico would be able to securely access the patient's records to learn what conditions he may have or what medications he takes."

The consortium started meeting on March 10 at the Pennsylvania Medical Society and hopes to have a statewide summit in Harrisburg this July to move the project another step forward. Details such as standardizing software and ensuring data security are important concerns for the group.

"We need to build an infrastructure that both patients and doctors can trust," said Tania Lyon, Ph.D., of the Pittsburgh Regional Healthcare Initiative. "The ability to coordinate care across different locations must be balanced by a guarantee of privacy to all patients. Medical data must be secure."

David B. Nash, M.D., chair of the Department of Health Policy at Jefferson Medical College in Philadelphia, adds, "This system is the future. And, it will benefit everyone – patients, doctors, hospitals, employers, and insurers. Look for it to revolutionize the American health care system."

# # #

Those organizations attending the consortium's initial meeting on March 10, 2005 included

AllHealth
Delaware Valley Healthcare Council
Geisinger Health System
Health Information Management Systems Society
Hospital & Healthsystem Association of Pennsylvania
Jackson Gastroenterology
Jefferson Medical College
KePRO
Loyalsock Family Practice
Medical Associates of the Lehigh Valley
Office of Pennsylvania Senator Jake Corman
Pennsylvania Academy of Family Physicians
Pennsylvania Department of Community & Economic Development, Office of Technology Investment
Pennsylvania Department of Health
Pennsylvania Department of Public Welfare
Pennsylvania Health Care Association
Pennsylvania Health Care Cost Containment Council
Pennsylvania Medical Society
Pennsylvania Patient Safety Authority
Pittsburgh Regional Healthcare Initiative
PMSCO Healthcare Consulting
Quality Insights of Pennsylvania
Temple University Hospital
University of Pennsylvania Health System
University of Pittsburgh Medical Center
University of Pittsburgh School of Health and Rehabilitation Sciences
Wellspan Health
West Virginia Medical Institute