Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

MARCH 31, 2009

Copyright PAeHI, 2009

Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Prepared For:

Pennsylvania Health Care Providers and Policy Makers

By:

The Pennsylvania eHealth Initiative and its Local Health Information Exchange Special Interest Group and Policy Committee

Edited By:

Executive Editor - Glen F. Marshall

Contributing Editor - Bob Mitchell

Copyright PAeHI, 2009

TABLE OF CONTENTS

Copyright PAeHI, 2009

EXECUTIVE SUMMARY

For a hospital, clinic, physician practice, nursing facility, or home-health organization considering whether to join a Health Information Exchange (HIE), one of the most important questions is "How does the HIE assure patient privacy and how will it help my organization do the same?" This white paper provides practical guidance to help you find the answer to that question and others like:

- Does the HIE provide a document that spells out the responsibilities of the HIE and of HIE participants?
- How does the HIE host assure that access to health data is limited to individuals who are authorized according to common privacy and security policies?
- How do organizations that contribute information to the HIE assure that they collect, store and communicate legally valid consumer consents for disclosure appropriately?
- How does the HIE host organization, data contributors, and data consumers transmit and store health information securely?
- What safeguards would ensure that only the minimum data necessary is accessed when the HIE use or access patient information for any reason beyond patient care?
- How do HIE hosts, data contributors, and data consumers use common interoperable security technology to assure confidentiality, integrity, authenticity, and accountability?
- How do HIE hosts protect and secure health information from possible theft or loss?

> We are all health care consumers. Each of us has an opinion on the value of health care privacy. Often this opinion is influenced by our own health condition (and whether we feel that our health condition has stigma associated with it). While patients universally want the best health care possible, most are unwilling to abrogate their rights to privacy. So, at its core, the issue is that each of us in good faith has a difference of opinion regarding what is appropriate privacy. The challenge is to design HIEs and clinical information systems to meet the public's reasonable privacy expectations, while still delivering health information as necessary for effective and efficient health care. *– John P. Houston, vice president, Privacy and Information Security & Assistant Counsel, University of Pittsburgh Medical Center*

Recommendations

This white paper supports recommendations stated in PAeHI's white paper ***Building a Sustainable Model for Health Information Exchange in Pennsylvania*** (February 22, 2008). The concepts indicated by italicized text are especially furthered by:

1. Design a mechanism for payers to support HIEs through a per transaction / usage fee model should be collaboratively designed with payer organizations and the state.

2. Empower a neutral organization with statewide collaborative capability to bring the diverse array of potential providers and consumers of HIE services to the table to *establish common standards for HIE-related value-added services*.

3. Commission research to assess the feasibility of public utility or public authority models to help finance HIEs which *meet minimum 'core' and/or value-added service standards*.

4. Realign provider payments over the long run to appropriately reward and *encourage use of HIE data* to avoid complications of chronic illness, and eliminate unnecessary, ineffective, or redundant care.

5. *Establish 'core' standards related to HIE implementation* using the same collaborative mechanism as described in #2 above for value-added services.

6. *Accelerate access to pharmacy-related data sources by HIEs* to promote accurate medication reconciliation.

7. Develop a mechanism by which a *single standard consolidated data set* would satisfy all provider-related State data reporting requirements; submission to one State agency and distributed by that agency to other departments or agencies as appropriate.

8. We further recommend that the State's approach to these and other areas of policy be consistent with the guiding principles laid out in ***Connecting Pennsylvanians for Better Health: Recommendations from the Pennsylvania eHealth Initiative*** (April 25, 2007), namely that:

    - Patients come first.
    - *Consumer privacy, security and confidentiality are paramount*.
    - *Multi-stakeholder collaboration* is essential.

> If you try to put together a network of hospitals and practices, nursing homes and home health, if they can't all trust that all of the different members of that network will use that information and protect the information appropriately, they won't participate. That's another level at which it's critically important that the system is designed in a way that is provably secure. The information is secure so that all of those different groups are willing to participate. – *James M. Walker, MD, FACP, chief health information officer, Geisinger Health System*

PAeHI recommends the robust patient privacy and security protections outlined in this paper, with priority given to the adoption of a common consent form governing patient data disclosure statewide. Collectively, these protections will help build and sustain the desired level of trust among patients, providers, Health Plans, and other stakeholders while balancing those protections with the necessity of adequate, accurate and timely patient data-sharing at the point of care.

Copyright PAeHI, 2009

INTRODUCTION

The Pennsylvania eHealth Initiative (PAeHI) was created in 2005 as a voluntary, public-private, non-profit (501(c)(3)) coalition to bring together Pennsylvania's healthcare and business stakeholders to develop a vision and a plan for the future of health information technology and the secure exchange of health information in Pennsylvania. The Hospital & Healthsystem Association of Pennsylvania, the Pennsylvania Medical Society, and Quality Insights of Pennsylvania provided early leadership and financial support. Governed by a representative board of directors, PAeHI offers a neutral forum for the health IT community to work together for a common mission—to improve patient care through the effective use of health information technology.

In the sharing of patient data, PAeHI recognizes that robust patient privacy and security protections are essential to build and maintain a necessary level of trust among patients, healthcare providers, health plans, and other stakeholders. PAeHI also believes that a balance must be maintained between the protection of patient privacy and the adequate and timely sharing of patient data at the point of care.

This white paper addresses healthcare data privacy and security for electronic information exchange. The key purpose is to help healthcare providers achieve acceptable data privacy and security assurance for healthcare consumers, while minimizing cost and confusion. It does not discuss the much broader issues of non-electronic healthcare data privacy or general security technology.

Future publications from PAeHI will provide updates as necessary to cover changes in privacy and security regulations as a result of the ARRA/HITECH bill, e.g. HIPAA and the Personal Health Record (PHR).

Patients in Pennsylvania have a right to private and secure health information. Everyone has the right to have their health information kept private and confidential and only shared with their healthcare provider. This ensures the patient/ provider relationship stays intact. To do so means keeping patient information secure via the necessary administrative, physical, and technical safeguards that ensure its confidentiality is maintained. Without these safeguards, this data is at risk of improper exposure.

It is also a matter of trust. Both patients and physicians must believe they can trust that their health information is protected, that it will only be used by or shared with those who have been authorized to do so, or those who have a legitimate need to know.
– Don Bechtel, Chief Privacy Officer, HDX, a part of Siemens Health Services, Siemens Healthcare

KEY DEFINITIONS

Concepts

Privacy
(1) The right to have all records and information pertaining to healthcare treated as confidential.

(2) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. (HIMSS, 2006)

Security
The means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. (HIMSS, 2006) The concepts of confidentiality, integrity, authenticity, and accountability are included in security.

ARRA
The American Recovery and Reinvestment Act of 2009 (also known as the Stimulus Bill), enacted into law on February 17, 2009.

HITECH Act
Title XIII (Health Information Technology) of ARRA may be cited as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act."

Stakeholders

Consumer
A person who obtains healthcare services or, by extension, a person who represents a patient such as a parent or legal guardian.

Patient
The direct recipient of healthcare and the subject of associated healthcare records.

Health plan
An entity that provides financial reimbursement to providers for their services to consumers and, in some cases, determines what and how much care will be reimbursed and how much consumers must pay.

HIE
Health information exchanges (HIMSS, 2006). A mechanism or organization designed to share healthcare information electronically across organizations within a region or community.

Provider
Any person or entity that supplies healthcare services for patients.

RHIO
A group of organizations with a business stake in improving the quality, safety, and efficiency of healthcare delivery. (HIMSS, 2006) A RHIO is an organization that provides the governance to develop and maintain an HIE.

Copyright PAeHI, 2009

Stakeholder
A general term includes all of the above plus vendors and government.

Personal Health Information

EHR
A longitudinal Electronic Health Record compiled from clinical data supplied by multiple care providers. It may be a single record or a series of records linked by a common patient identity.

E-Prescription
A prescription that is sent from a prescriber to a pharmacist according to electronic transaction standards, e.g., NCPDP Script or HL7, rather than written form. A Fax is not an e-prescription.

PHR
A Personal Health Record generally created, maintained, and controlled by a consumer with some supplementary material from care providers. It may be a physical electronic record, e.g., on a USB key, or stored remotely in an online repository on the consumer's behalf.

Protected Health Information (PHI)
Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Protected Health Information (PHI) is any information, whether oral or recorded in any form or medium that is created or received by a covered entity, is used to identify an individual and relates to the individual's past, present or future physical or mental health; the provision of health care to the individual; or the past, present or future payment for health care. The HIPAA privacy and security rules specify the protections.

Key Staff

Privacy officials
The HIPAA privacy rule requires each covered entity to designate a "privacy official" responsible for developing and implementing the necessary policies and procedures for compliance. While some familiarity with technical topics may be helpful, this position is largely policy-focused. Covered entities must also designate a contact person or office for providing information, receiving complaints, and administering of consumers' health records rights for the following:

- Access
- Amendment
- Disclosure accountings
- Supplemental protections
- Confidential communications
- Authorizations for additional uses

Security Official
The HIPAA security rule requires covered entities to designate a "security official," responsible for developing and implementing the necessary policies and procedures for compliance. This position requires technical knowledge to adequately determine and implement the required protections.

Copyright PAeHI, 2009

The healthcare industry has been spirited, if not passionate regarding privacy and security from both the provider and patient perspective. The issues surrounding privacy and security continue to challenge all stakeholders, particularly those involved in the delivery of care. Looking at privacy in the security landscape will always be a challenge because the patient relies on someone else (providers) to interpret personal information about their care and treatment options. Yet many would agree that you cannot have privacy without security, nor security without privacy. On the other hand, security in the privacy landscape varies by technology solutions, approaches and attempts to meet regulation, standards and best practices.

United States National Landscape

An estimated 18.5% of medical privacy complaints lodged with the Department of Health and Human Services resulted in changes in behavior by healthcare organizations since the department started its HIPAA enforcement program in April 2003 (Melamedia LLC, 2008). In September 2008, the Government Accountability Office reported that HHS efforts to protect patient health information had undergone many different initiatives that are contributing to the development of a successful privacy approach. This included setting milestones, ensuring HIPAA privacy issues are addressed, and tackling challenges with the nationwide exchange of patient care information. Although still a work in progress, the Office of the National Coordinator for Health Information Technology (ONC) is working through the challenges with the Healthcare Information Technology Standards Panel (HITSP), the Certification Commission for Healthcare Information Technology (CCHIT), and State Level Initiatives through the State Alliances for eHealth.

The intent of Health Information Exchanges (HIEs) outlined in the National Framework was to provide architecture, processes, and procedures to give providers access to relevant information for treating their patients. Many HIEs have taken the position that HIPAA is not a legal barrier to exchanging information for the direct care of patients. Other measures used by HIEs include Business Associate Agreements and consumer consents for disclosure. While consistency does not yet exist, no HIE has been charged with violating HIPAA privacy or security regulations. The full picture is not complete at the state levels, as some states have additional privacy requirements under development.

Regulations

At the U.S. national level, healthcare information exchange is subject to a variety of regulatory controls. These include:

- Health Insurance Portability and Accountability Act privacy and security rules (HIPAA, 45 CFR Parts 160, 162, and 164) which broadly protect healthcare data from misuse.
- Alcohol and Drug Abuse privacy rules (42 CFR Part 2), with added patient privacy for certain federally funded treatment programs.

Copyright PAeHI, 2009

- Patient Safety and Quality Improvement rules (42 CFR Part 3) for aggregation and analysis of patient safety events, Subpart C privacy and security protections
- Family Educational Rights and Privacy Act (FERPA, 34 CFR Part 99) generally classifies school health records as education records which cannot be shared without consent.1
- The FTC "Red Flag" rule (16 CFR Part 681), as it applies to medical identity theft. The enforcement date for this has been delayed until May 1, 2009.

In December 2008, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published a "Privacy and Security Framework and Toolkit," designed to establish privacy and security principles for stakeholders engaged in the electronic exchange of health information and includes tangible tools to facilitate implementation of these principles.

In addition, the American Recovery and Reinvestment Act of 2009 (ARRA, also known as the Stimulus Bill), which was signed into law on February 17, 2009 (the "Effective Date"), includes significant changes to healthcare privacy and security protections. Most of these changes are in the section of the law known as the HITECH Act. HHS has until December 31, 2009 to publish various sets of regulations that will flesh out the legal provisions in the new law, but a number of provisions of the HITECH Act went into effect immediately on the Effective Date, including:

- Section 13410 established increased tiered civil penalties for HIPAA violations, ranging from $100 per violation up to $50,000 per violation, with an annual maximum amount of $1.5 million in any calendar year for violations of the same requirement.
- Section 13410 also allows state attorneys general to initiate civil actions for the first time and collect damages for HIPAA violations affecting its state residents.
- Section 13408 clarifies that HIEs and RHIOs are business associates of covered entities.

In addition, some of the other significant changes that the HITECH Act will make to HIPAA include:

- Business Associates will be directly subject to parts of the HIPAA privacy and security rules, including civil and criminal penalties and sanctions for violations.
- Adding Federal privacy breach notification requirements for covered entities, business associates and commercial PHR vendors.[2]
- Adding restrictions on the marketing and sale of patient data.
- Narrowing HIPAA's broad exclusions for healthcare operations.

[1] The Departments of Education and Health and Human Services recently released guidance to explain the relationship FERPA and HIPAA and to address confusion about how they apply to student health records. (U.S. Department of Health and Human Services and US Department of Education, 2008)

[2] Although a number of commentators interpret the HITECH Act as covering PHR vendors such as Google and Microsoft, Google spokesmen have been quoted as saying that neither the HITECH law nor HIPAA have any applicability to Google Health. "Google Says New Privacy Rules Don't Affect Its PHR," ModernHealthcare.com, March 4, 2009). As of the date this paper was completed, this issue has not been resolved.

- Adding requirements to account for all disclosures from EHRs, *including* TPO (treatment, payment and healthcare operations).
- Requiring all uses, disclosures or requests of PHI to be limited to the limited data set or, if needed, the minimum necessary to accomplish the intended purpose.
- Improving enforcement and adding personal accountability for violations.

While the above are key principles, other Federal and state laws and regulations also govern general data privacy. The theme is consistent: act rationally and protect private information consistent with the risks, and do not wait until regulatory sanctions force changes.
These laws, regulations, and legal precedents generally apply to the:

- Holder of the data
- User (requester) of the data
- Data itself
- Purpose of the use or disclosure of the data
- Timing of the use and disclosure of the data
- Methods and mechanisms used to collect, maintain, use and disclose data

Up to this point, the Personal Health Record (PHR) privacy and security has not been subject to regulation. However, there is ongoing discussion regarding PHRs and this regulation. The applicability of new PHR provisions under the ARRA is unclear in the absence of regulatory provisions that are yet to be defined. PAeHI recommends that the reader access the HIMSS web site for the most current updates regarding the ARRA/HITECH: www.himss.org.

Current statistics published by OCR indicate that about 18.5% of medical privacy complaints lodged with the Department of Health & Human Services resulted in changes in behavior by healthcare-related organizations since the Department began its HIPAA enforcement program in April of 2003. Enforcement actions may occur in a variety of methods. Covered entities have primary responsibility to prevent, discover, and mitigate privacy breaches. When that process fails, the Federal agencies will intervene to remedy the situation. Except in a handful of cases, the Justice Department has been extremely reluctant to act in cases involving HIPAA violations. In addition, U.S. courts have generally supported the right of patient privacy in healthcare, except in certain well-defined cases where Federal or State governmental interests prevail. Other U.S. privacy protection laws and regulations exist. While they may apply to an HIE's particular circumstances, they are not within the scope of this paper.
Additional regulation is likely within the next two years:

- In September 2008, the GAO published a report recommending that HHS include in its overall privacy approach a process for ensuring key privacy principles and challenges are completely and adequately addressed. In written comments on a draft of this report, HHS generally agreed with the information discussed in the report.
- Well-funded healthcare information technology proposals from President Obama and Congress are expected. These are likely to include strengthened privacy and security provisions.

- Significant concerns about consumer privacy persist. Healthcare is likely to be impacted by impending legislation and regulatory actions. The FTC "Red Flag" rule is an example.

Ongoing Standards Work

The Office of the National Coordinator for Health Information Technology (ONC) is sponsoring technical standardization with the Healthcare Information Technology Standards Panel (HITSP), and the Certification Commission for Healthcare Information Technology (CCHIT).
While there is much focus on the Federal and state regulatory requirements, efforts for significant enabling technology solutions for privacy and security is overseen by ONC. HITSP and CCHIT are key organizations to monitor in healthcare IT strategic and tactical planning and for developing product-purchase plans, as they incorporate other organizations' standards in their work products.

Table 0-1 Healthcare IT Standards Organizations Timeframe

Standards Development	Standards Usage Specification	Standards Implementation
3-5+ Years	**2-4 years**	**Immediate to 18 months**
ASTM E31[3] HL7 Security WG[4] ISO/TC 215 WG4[5] OASIS XSPA[6]	**HITSP**[7] NeHC[8] IHE[9]	**CCHIT**[10]

HITSP and CCHIT are the key organizations to watch in healthcare IT strategic and tactical planning and for developing product-purchase plans. All of the other listed organizations' standards and other work-products are being incorporated and used in their work products.
To exchange data with government healthcare, in particular the Department of Defense and Veterans Administration, healthcare providers must also conform with the Federal Information Security Management Act of 2002 (FISMA) in accordance with SP 800-53 (Ross, Katzke, Johnson, Swanson, Stoneburner, & Rogers, 2007). Compliance with this act is actively audited. There are very tight security controls on the disclosure and use of active duty military health data, which is a Federal national security requirement.

[3] ASTM International, Health Informatics Committee. See http://www.astm.org
[4] Health Level Seven, Security Workgroup. See http://www.hl7.org
[5] International Organization for Standardization, Healthcare Informatics Technical Committee, Security Workgroup. See http://www.iso.org
[6] Organization for the Advancement of Structured Information Standards, Cross-Enterprise Security and Privacy Authorization Technical Committee. See http://www.oasis-open.org/committees/xspa
[7] Healthcare Information Technology Standards Panel. See http://www.hitsp.org
[8] National eHealth Collaborative. See http://www.nationalehealth.org
[9] Integrating the Healthcare Enterprise. See http://www.ihe.net
[10] Certification Commission for Healthcare Information Technology. See http://www.cchit.org

Marketplace

The Connecting for Health collaborative has nine privacy principles in its framework. (Connecting for Health, 2006) In summary, they are:

- Openness and Transparency: There should be a broad and universal practice of transparency in the way data is handled. Purpose, Specification and Minimization: Data should never be collected without people knowing that it is being collected. Collection Limitation: The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of persons. Use Limitation: Reuse (of data?) should not be permissible without explicit consent of individuals.
- Individual Participation and Control: Individuals are key participants in processes of information collection and dissemination, and not as mere subjects or passive spectators.
- Data Integrity and Quality: Mechanisms need to be developed to address risks to data integrity, accuracy, completeness, and timeliness and for establishing accountability among those who maintain records.
- Security Safeguards and Controls: Reasonable security safeguards should be built to protect against loss, unauthorized access, destruction, use, modification, or disclosure of personal information and breaches should be reported immediately to the affected stakeholders.
- Accountability and Oversight: Mechanisms should be built to ensure that the responsibility for privacy violations is identifiable, and that remedial action can be taken.
- Remedies: Clear legal remedies exist to address and correct violations of the above privacy principals, including statutory punishments.

On October 10, 2008, an article in the Wall Street Journal (Gupta, 2008) discussed trends toward large-scale network communications for healthcare, providing remote and offshore medical and non-medical services employing individual healthcare data. This includes specialist consultations where patients do not need to be seen in person, e.g., radiology, remote monitoring in low-acuity care, pharmaceutical adverse event reporting and tracking, and continuing medical education (CME). Healthcare organizations that do not take advantage of these trends will experience competitive and cost disadvantages, as has happened in other industries. Necessary privacy and security protections are part of this.

A recent eHealth Initiative webinar (Bordenick, McGraw, Williams, Rosati, & Posnack, 2008) noted the following:

- Use of Electronic Health Records (EHR) by providers and health plans is increasing.
- Provision of consumer-controlled Personal Health Records (PHR) through employer, vendor, and healthcare provider channels. This addresses the consumers' desire to access and control their healthcare but raises significant concerns about privacy.

- Network based data sharing via HIEs and RHIOs. These types of organizations are not covered entities under HIPAA, suggesting the need for new legislative and regulatory actions to protect patient privacy and security.
- The Connecting for Health Common Framework (Connecting for Health, 2006) provides a roadmap for planning healthcare IT evolution and developing privacy policy with technology choices.
- There is an emerging requirement for use of formal patient consent for sharing data, beyond the provider-voluntary consent in HIPAA and the drug and alcohol treatment program requirements in 42 CFR Part 2. The form and content of such consents is not defined uniformly. Consents are already defined by some states, leading to regulatory conflicts when data might cross a state border. The Health Information Security and Privacy Collaborative (HISPC) has recommended that a standard template for consents be developed and implemented.
- There is minimal stakeholder consensus on the uses of security technology in healthcare, and expectations often exceed what is realistic and affordable.

The emergence of clinical genomics raises novel privacy issues. For example, a clinically relevant finding from a person's genome implies similar findings in his family. Privacy policies that obtain permission to use and communicate such data are not well defined. Additional protections are required from legislative and regulatory action.

The recent Healthcare Information and Management Systems Society (HIMSS) 2008 study reveals that, while basic technical security controls are in-place for most providers:

- More than half of the responding organizations dedicated less than three percent of the overall IT budget to information security. More sophisticated security technology, such as single sign-on and encrypted e-mail, are frequently identified as part of future plans.
- Nearly all respondents shared data electronically and nearly half of these organizations used additional security controls beyond the basic ones.
- Respondents did not consider the threat of medical identity theft at their organization as being that high, and only 20 percent reported an incident at their organization. However, most have changed their business practices to mitigate the threat.

The HIMSS Privacy and Security Steering Committee recommends implementation of strategic initiatives that promote the privacy and security of healthcare information and management systems. They have set the following goal: "By 2014, all entities who use, send, or store health information meet requirements for confidentiality, integrity, availability and accountability based on sound risk management practices, using recognized standards and protocols." In support of this goal, HIMSS has launched several work groups that are actively involved with industry changing activities to achieve this goal.

Pennsylvania

The Pennsylvania eHealth Initiative (PAeHI) presented a white paper "Building a Sustainable Model for Health Information Exchange in Pennsylvania" to the Governor's Office of Health Care Reform in February 2008 as a framework for the adoption of a statewide HIE. The recommendations included key concepts for which privacy and security protects are required or directly relevant:

- Encourage use of HIE
- Have a single standard consolidated data set
- Enable multi-stakeholder collaboration
- Accelerate access to pharmacy-related data sources
- Ensure privacy, security and confidentiality of healthcare data
- Establish common standards for HIE-related value-added services.
- Define minimum 'core' and/or value-added standards.

Pennsylvania Department of Health regulations related to hospital-held information state:

> § 115.27. Confidentiality of medical records. All records shall be treated as confidential. Only authorized personnel shall have access to the records. The written authorization of the patient shall be presented and then maintained in the original record as authority for release of medical information outside the hospital.

The Pennsylvania Breach of Personal Information Notification Act, 73 PS 2301 (Pennsylvania General Assembly, 2008), broadly establishes privacy requirements for all businesses and government entities, not just healthcare. It requires the subject of data, such as patients, to be notified without unreasonable delay when the business reasonably believes that their personal information may have been disclosed to unauthorized people. There are no exceptions for immaterial breaches but encrypted, redacted, or publicly available government data are excluded. The notification provisions are enforced by the state Attorney General, with no private right of action. However, affected people may still press for damages via separate civil actions.

Other provisions in Pennsylvania include (Pritts, Choy, Emmart, & Hustead, 2002):

- Consumers may obtain a copy of their medical records, with a copying fee, including records maintained by health plans.

- Data used for research requires consumer consent for disclosure and is to remain anonymous to the greatest extent possible.

- Health plans and utilization review entities must have procedures to ensure all identifiable information regarding enrollee health, diagnosis and treatment is

adequately protected and remains confidential in compliance with all applicable Federal and state laws, regulations, and professional ethical standards.

- Mental health care professionals may not, in any civil or criminal matter, disclose confidential health information acquired from the client in the course of professional services. This includes providers, guidance counselors, school nurses, home and school visitors, and school psychologist-students.

- All patient records prepared for state and local programs for drug and alcohol abuse treatment may not be disclosed without the patient's consent, except in emergencies.

- Providers or social services may not disclose confidential HIV-related information without the patient's written consent.

- A physician may not disclose, in a civil proceeding, information he/she acquired caring for a patient that tends to blacken the character of the patient.

- Patients must be notified without unreasonable delay when a provider believes that their personal information may have been disclosed to unauthorized persons.

- Hospitals and laboratories must report cases of cancer to the Department of Health, but the information is confidential and not open to public use.

- Physicians must report persons who have, or who are suspected of having, a communicable disease to the local board or department of health. This also includes clinical laboratories, orphanages, childcare group settings, and institutions maintaining dormitories and living rooms.

Pennsylvania does not currently have specific protections for genetic data, distinct from other healthcare data.

Benchmarks from Other States

Comprehensive and authoritative data comparing Pennsylvania with other states' provisions for healthcare privacy and security are scarce, at least from publicly accessible sources. There are, however a variety of anecdotal sources.

Across the Unites States, State legislators introduced more than 370 bills to boost healthcare information technology over an 18-month period in 2007 and 2008, with more than a third passing. The volume of IT legislation introduced was three times higher than in a similar period from 2005 to 2006, the conference said. (National Conference of State Legislatures, 2008)

Accelerating Progress: Using Health Information Technology and Electronic Health Information Exchange to Improve Care (State Alliance for eHealth, 2008) examined the challenges states face in implementing HIT and HIE, including concerns about data privacy and security such as:

- The trade-off between addressing risks to privacy and risks to patient care quality, safety and cost.
- Inconsistent application of privacy policies among healthcare providers and HIEs, leading to mistrust.
- Inconsistent data-sharing privacy protections among states.

The Alliance recommends the following strategies:

- Consolidate and update relevant privacy and security laws to better respond to consumer protection needs in an electronic exchange environment among care providers.
- Educate leaders and support efforts to reduce variation of US State and Federal privacy requirements while ensuring appropriate consumer protections.

The following information from other states provides benchmarks for possible future changes in Pennsylvania:

- On September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation established significant new regulations, *201 CMR 17.00: Standards for The Protection of Personal Information*, which affect how all Massachusetts organizations protect confidential data. It requires explicit policies for employee access to data, immediately denial of access to terminated employees, written certification of compliant privacy practices from vendors, detailed document-tracking for health records, monitoring to detect unauthorized access, and encryption of all data stored on portable electronic devices.
- In September, 2008, California enacted two new privacy relevant laws (Conn, 2008). They define "unauthorized access" as "the inappropriate review or viewing of patient medical information without a direct need for medical diagnosis, treatment or other lawful use." These laws effectively extend HIPAA privacy and security rules requirements to all entities. There are civil penalties -- $25,000 for the first violation and $17,500 for each subsequent one -- on individuals or entities that improperly disclose private medical information, in addition to penalties that may be imposed for HIPAA violations. Requirements of the existing individual right of action, have been relaxed, so that the plaintiff does not have to show that he or she "suffered or was threatened with actual damages," only that negligence occurred. Any facility that fails to report unlawful or unauthorized patient privacy breaches is also subject to penalties. The California Office of Health Information Integrity acts as the watchdog.
- California has a major initiative called the California Privacy & Security Advisory Board (CalPSAB – see http://www.ohi.ca.gov/calohi/PSAB/). CalPSAB is an initiative from the Governor's office, which reports to the Secretary of Ca DHHS. It is funded in part by DHHS funds, and part by round 2 funding from the national HISPC project. The charter of CalPSAB is to adopt a set of standards for privacy and security for the

state, and then to put together implementation specifications that will make the health data sharing processes uniform within California. Minnesota (Golden, 2008) requires a written consent for nearly all disclosures – including treatment – and they expire within a year. Severe penalties, and an individual right of action, exist for inappropriate disclosures. The disclosure requirements have recently been updated (Minnesota Office of the Revisor of Statutes, 2008) to facilitate electronic data exchange, include recordkeeping to track when and to whom a patient's data, and which records, were disclosed.

- New Jersey has privacy laws that protect the privacy of patient health information beyond HIPAA. They vary based upon the type of information shared by care providers, e.g., genetic data and information relevant to Sexually Transmitted Diseases and HIV. In addition, certain provisions require explicit patient release and consent. New Jersey Hospital Licensing Standards and facility laws for acute, ambulatory or skilled nursing care facilities also govern and the patient privacy rights and consent for disclosure.
- New Hampshire law prohibits the sale of doctor-specific prescription data. This was recently upheld by a Federal appellate court in Boston. The court said that the state had made a compelling case that barring such data mining would help reduce the cost of healthcare. Vermont and Maine, in the same appellate district, have similar laws in the works. This decision should open the door for those laws, and may also encourage other states to pass similar laws preventing the practice of selling the data. (New York Times, November 18, 2008)
- The Rhode Island Health Information Exchange Act of 2008 establishes the rules governing the state-wide exchange. The law gives patients control over who sees their records, puts the Health Department in charge, requires a commission to oversee the exchange and sets civil and criminal penalties for violating the law. Provisions of the law were recommended by the Rhode Island Quality Institute, the private agency designated by the state to run the information exchange.
- Vermont law 2007 VT H 229, enacted in June 2007, promotes the use of national standards for the development of an interoperable system, which shall include provisions relating to security and privacy. (National Conference of State Legislatures, 2008)
- The majority of states have taken steps to safeguard genetic information beyond the protections provided for other types of health information. Genetic information can predict familial health information beyond the individual patient, and thus affect the privacy of a patient's genetic relatives. (National Conference of State Legislatures, 2008)

WHAT IS ACTUALLY REQUIRED

As described above, covered entities are subject to a number of state and federal laws related to security and privacy of health information, as well as various organizational and contractual requirements. These existing laws and policies contribute to the privacy and security framework of a Health Information Exchange. However, knowing their scope and limitations, it is important to dispel common misunderstandings and provide guidance to healthcare providers about what they are actually required to do.

The most critical element is that whatever the size of your healthcare organization, whether a one-person practice or a multiple-hospital chain, that you think about and address the particular risks you face. One cannot make "one-size-fits-all" policies, and it is necessary to fit the solutions, procedures, and tools to the situation at hand.

Dispelling the Myths

Here are some common myths associated with healthcare privacy and security:

- **Myth:** It is required to audit all accesses to patient data (i.e., record who saw which records).
  The truth: The HIPAA security rule only mentions security audits but does not define their content.
  Advice: It is a good idea to audit all accesses, following HITSP specifications, as future privacy regulations may require it.
- **Myth:** Retain security audit records for 6 or more years.
  The truth: HIPAA says nothing about security audit record retention.
  Advice: This is an organizational policy decision, based on risk analysis and cost.
- **Myth:** Passwords must be a minimum of 8 characters long with upper & lower case alpha plus one or more numbers.
  The truth: The HIPAA security rule briefly mentions the need for password management but does not define any specific requirements.
  Advice: This is an organizational policy decision, based on risk analysis.

  Myth: It is required to report all accesses to consumers' health data if they ask.
  The truth: The HIPAA privacy rule requires tracking of all access other than those for treatment, payment, or health care operations – which are by far the most frequent ones. However, under the HITECH Act, all disclosures of PHI made "through an EHR," even for TPO, must be accounted for during the three year period prior to the date of the request. Keep in mind that this applies only to disclosures outside of the organization, not uses within the entity. Also, the accounting period has been reduced from six years to three years.
  Advice: Keep a manual or automated record of reportable disclosures. Do not depend on security auditing to do this. Provide a report from it to consumers upon request.

Copyright PAeHI, 2009

- **Myth:** Covered Entities should only deal with IT vendors who are or claim to be HIPAA compliant.
  The truth: Before the passage of ARRA, IT vendors that dealt with individually identifiable health information were only indirectly subject to HIPAA, by way of the contractual obligations set forth in a business associate agreement. Under the HITECH Act, business associates will be directly subject to specified sections of the HIPAA privacy and security rules, including civil and criminal penalties and sanctions for violations; however, they will still need to enter into business associate agreements to insure compliance with other obligations under HIPAA.
  Advice: Have a well-constructed business associate agreement with every IT vendor, and periodically audit their compliance with it.

- **Myth:** A notice of privacy practices must be signed by a consumer for every visit.
  The truth: The HIPAA privacy rule requires a notice of privacy practices be provided by health care providers to a consumer at the first time of service, and it is valid from then on, unless material changes are made. Health Plans must distribute the notice at least once every three years.
  Advice: Obtain a signed notice on a patient's first visit and include it in their medical record.

- **Myth:** Lack of standards for privacy and security
  The truth: We have all the technical standards we need. (Halamka, Interoperability Advice for the New Administration, 2008) What we lack are coherent *policies* -- laws, regulatory, organizational -- to define and establish trustworthiness in healthcare IT. Clear and unambiguous policies, plus ways to reconcile multiple policies that may apply to a given situation, will enable existing IT standards to be effective.
  Advice: Promote the convergence of policies with legislators and regulators, and establish common-policy trust agreements among healthcare providers.

> The privacy and security of PHI are key elements to the adoption of HIE, which in turn will make HIE successful. If patients are unsure that their data will be shared confidentially, they will have the option to opt-out of the HIE and doctors will have incomplete information. It will be critically vital to the project that the patients' trust is obtained from the beginning. If that trust is broken, the burden will lie solely on the healthcare providers to regain the confidence of the patients, and that could be extremely costly. – *Kathryn J. Magar, manager, information security, Wellspan Health, York, Pa.*

Policies: Legal, Regulatory, Organizational, and Personal

Effective privacy and security protections start with clear and unambiguous policy definitions. Systems and networks that are assembled with no reference to a consistent policy framework are likely to have significant exposures to privacy and security breaches.

While legal requirements form a broad policy envelope, there must also be agreements among HIE participants, providers' policies, and patient-specific disclosure consents and restrictions.

Trust Agreements Among Care Providers

The parties associated with HIEs should establish a framework of trust. This is based on written agreements that include accountability, standards, responsibilities, and procedures for:

- Administration
- Accountabilities
- Data ownership and stewardship
- Data integrity
- Data quality
- Data use and disclosure
- User/entity identification
- User/entity access control
- Patient/data-subject identification
- Technical interoperability
- User/entity training

The 2008 NHIN-HISPC-SLHIE Joint Conference (American Health Information Management Association, Foundation of Research and Education, 2008) reviewed previous work and proposed a common approach to developing information exchange policies and model agreements covering:

- Communication requirements - supplying a reason for "no return of health information"
- Data content/quality requirements - Summary records
- Consumer permissions, consent process including managing multiple consent directives and resolving different levels of authentication and auditing
- Routing of data
- Response to a security incident, including mandatory and non-mandatory notification of breaches plus audit logs

A sample trust agreement now used in Pennsylvania is included in the Appendix.

Consumer Consent for Disclosure[11] of Health Information

Most consumers want healthcare systems in which all of their health information is available to the people and groups and facilities they choose to care for them. All of our privacy and security efforts need to support this widely felt need. That is, the vast majority of consumers want to control their healthcare information by delegating that control to people and organizations they trust. This does not mean that robust safeguards are not needed, but it does mean that the system needs to be simple enough for consumers to use. Under the HIPAA

[11] The HIPAA Privacy Rule has used the term "authorization". This has a different meaning for Security. To prevent confusion, HITSP uses "consent for disclosure" or just "consent".

privacy Rule, information may be disclosed for treatment, payment, or operations without prior consent from the consumer. In addition:

- Healthcare providers must (except in an emergency) obtain the consumer's written acknowledgment of receipt of the notice of privacy practices. It is not necessary to obtain their consent.
- A consumer may request restriction on disclosures of Protected Health Information for treatment, payment, or health care operations. If the provider agrees to the restrictions, it must comply except in emergencies.
- A provider must accommodate consumers' reasonable requests for communication alternatives, e.g., not using their home mailing addresses, certain telephone numbers, or e-mail addresses.

In conformance with the HIPAA privacy rule, healthcare providers must obtain the consumer's signature on a notice of privacy practices indicating that they have read it. It is not necessary to obtain their consent. This acknowledgement is often included in other paperwork, e.g., consents for treatment. It is best to keep it simple, stating the policies for sharing healthcare information and communicating a balance between providing necessary care and patient privacy.

Other uses of protected health information require a written consent with these elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health

> One of the things I've seen is that there has not been an easy way when you are exchanging or working in a connected network to be able to tell or notify the rest of the participants as to the preferences of the patients, regarding information exchange. We had to do custom programming for every single hospital that participates today in order to be able to send flags to the exchange to indicate whether or not that patient has authorized access to their information. If there were a national standard and system requirements for certification, then it would be much easier to exchange. I think we are moving in that direction with CCHIT and HITSP standards today. *– Jim Younkin, IT program director, Geisinger, Health System, project director, Keystone Health Information Exchange*

information for research, including for the creation and maintenance of a research database or research repository.

- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

For federally-funded drug and alcohol abuse programs, a consent form is required for all disclosures that explicitly identifies the patient as a substance abuser. Other clinical data, e.g., comorbidities, may be disclosed in accordance with the HIPAA privacy rule. Minors must even sign a consent form before information is disclosed to their parents. The consent must include the following elements:

- Name or general designation of the program or person permitted to make the disclosure
- Name or title of the individual or name of the organization to which disclosure is to be made
- Name of the patient
- Purpose of the disclosure
- How much and what kind of information is to be disclosed
- Signature of consumer (and, in some States, a parent or legal guardian)
- Date on which consent is signed
- Statement that the consent is subject to revocation at any time except to the extent that the program has already acted on it
- Date, event, or condition upon which consent will expire if not previously revoked

In addition, drug and alcohol abuse programs must comply with these HIPAA privacy provisions:

- Ensure that the consent complies with the applicable HIPAA requirements in 45 CFR §164.508.
- Programs must give consumers a copy of the signed form.
- Programs must keep a copy of each signed form for six years from its expiration date.

Under HIPAA, written revocation of consent for disclosure is required. But under Drug and Alcohol provisions, oral revocation is sufficient.

Because of significant attention being brought to patient privacy issues, it is prudent to prepare for stricter regulatory requirements. This includes these areas:

- Direct and secure consumer access to their EHR data and request amendments to it
- The choice of opt-in or opt-out for disclosure
- Additional elements to be added to the notice of privacy practices
- Tracking of routine disclosures that are now excluded from tracking by the HIPAA privacy rule

- Mandatory consumer-directed privacy consent controls to limit or prevent disclosures to specific individuals or organizations
- Additional disclosure requirements and prohibitions for special categories of data, e.g., mental health, substance abuse, HIV…
- The handling of genomic data, including protecting the privacy of patients' relatives
- New responsibilities placed upon consumers, e.g., for PHRs
- The need for a notice of possible clinical consequences of consumer-initiated redactions of health information
- Retroactivity – withdrawing consent for disclosure and methods to request previous disclosures to be deleted
- Notifications of breaches and remedies
- Individual right of action for unauthorized disclosures

While there are many calls for a national framework and a consistent approach to privacy protections among the states, it is too early to predict the likelihood or extent of success. In the meantime, some stakeholders look to leverage HIE policy as a mechanism to introduce new privacy protections and, as detailed previously, a number of states have already enacted policies or laws that "raise the bar" above the current legal requirements. In Pennsylvania, Health Information Exchange initiatives will be faced with the challenge of balancing the needs of privacy advocates and healthcare providers as they develop policies and procedures related to patient consent and control.

Sample patient consent forms now used in Pennsylvania are included in the Appendix.

Business Associate Agreements

The HIPAA privacy rule requires that healthcare providers have business associate agreements with their providers. The legal requirements are beyond the scope of this paper. PAeHI urges providers to consult an attorney before preparing or signing one. Sample business associate agreements now used in Pennsylvania are in the Appendix.

The ARRA adds compliance requirements for business associates, including privacy breach notification and penalties for violations. It also includes HIEs and RHIOs as business associates. The ARRA requires business associate agreements to include these requirements. As of this writing it is unclear if, or how, the new ARRA provisions applies to existing agreements.

Risk management[12]

To identify and make good business decisions about privacy and security requirements, health care organizations must perform security risk assessments, privacy risk assessments and business risk assessments. This must be done on an ongoing basis, as healthcare IT exists in an

[12] This section is derived from HITSP TN900 – Security and Privacy Technical Note, version 1.2 (2008)

environment which is constantly identifying new issues and risks, but not limited to the security domain. In particular, security risk assessments are required under the HIPAA security rule.

It is important to understand the business or healthcare delivery relevance of the risks identified, how much risk is acceptable, what types of risk may arise from new technologies, and how much to spend on mitigating risk. A thorough risk assessment includes different types of risks including IT security, privacy, safety, loss of access to IT-based services and data resources, corporate risks, and human error factors. This enables risks to be properly considered when determining technology strategies and tactics.

Risk management provides a cohesive vision to prevent unwise investment in security, privacy or other technologies based on popular demand, sales presentations, and sensationalist press report. It is about much more than keeping hackers from stealing personal health information. Rather, it is critical to address such issues as:

- Protecting confidentiality of personal information
- Legal compliance
- Safe provision of healthcare services
- Patient safety
- Avoiding medical errors
- The cost and benefit of protective measures

While the majority of risks can have negative impacts, risk analysis can expose opportunities to enhance the quality of care, for example, by reducing wait times, providing consumers with access to their health data, and reducing medication conflicts through automated checks against a database.

Effective risk management enables senior management, middle management, and the technical and operational staff to:

- Improve business performance by informing and improving decision making and planning
- Promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities is encouraged
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance
- Assist in meeting healthcare requirements and objectives
- Facilitate partnerships with other healthcare organizations to address the issues inherent in interoperable systems and data sharing
- Benefit patients who often receive care from multiple healthcare providers by effective information sharing to improve the safety and quality of healthcare services

Risk Management Framework

A risk management framework combines all the processes involved in realizing existing as well as newly identified opportunities in a manner consistent with public interest, human safety and the law, while managing adverse effects caused by the complexity of healthcare systems. It involves identifying, assessing and judging risks, assigning ownership, taking action to mitigate or anticipate them, and monitoring and reviewing progress. The outcome is a holistic analysis that weighs the cost of protective measures and establishes a continuous process to manage them.

A risk management framework's complexity needs to match the scale and scope of a healthcare organization. Large-scale organizations may employ professional risk analysts or consulting firms; smaller organizations may use cookbook-like tools. For example, the risks posed in an HIE with 7,000 end-user devices are multiplied in their potential impact far more than a small physician's practice with 3-4 PCs.

The key tools in a risk management framework identify risks, the financial consequences, and the likelihood of risks occurring. They are used continually, not just at the beginning of a project. The tools employed can be a simple spreadsheet up to a formal analysis process, depending on the size and scope of a healthcare organization.

In contrast, an ad-hoc approach to addressing newly identified risks may overlook the importance of existing risks. It creates new risks such as technology conflicts, obsolescence, and inadequate focus on prioritizing solutions according to greatest value. It can also waste time and money, e.g., acquiring expensive security technology to address a low-probability risk. Instead, there must be an organization-wide commitment to applying the risk management framework on a continuous basis. This is the proven method of benefiting from risk management activities.

Organizational risk assessments help decision makers define and map long-term security strategies, which may identify requirements for adopting new technologies as part of an overall security strategy. These are tailored towards specific compliance requirements such as HIPAA or fulfilling the requirements under the guidance of a security operational framework standard such as ISO 27799 (International Organization for Standardization, Technical Committee 215, 2006). Documented techniques and methodologies exist for conducting organizational risk assessments, which draw from relevant best practices and industry guidelines or requirements such as NIST SP 800-53 (Stoneburner, Goguen, & Feringa, 2002).

System specific risk assessments are often geared towards specific compliance requirements and are designed to help organizations understand the risks associated with implementation of a specific system or technology. They usually include detailed, in-depth analysis of all aspects of the information system under review, including relevant areas of the system development life cycle and appropriate security best practices for information systems. An in-depth system risk

assessment will help organizations to better understand any additional risk as a result of implementing new technologies, and allow them the opportunity to make configuration changes or additional mitigation measures to reduce the risk to an acceptable level prior to deployment.

Identifying Threats

A good starter set of security threats may be found online in NIST SP 800-30 (Stoneburner, Goguen, & Feringa, 2002). These are common threats for all IT systems.

Healthcare has some particular threats not found in other IT systems:

- Medical data, particularly that which is based on claims, may be used to profile patients and negatively impact non-medical aspects of patient's life such as employability, credit, and life insurance purchasing.
- Medical identity theft is the misuse of another individual's identification such as name, date of birth, Social Security Number, or insurance policy number to obtain or bill for medical services or medical goods. In addition to financial loss, medical identity theft may include inappropriate treatment of patients, leading to liability claims. While compliance with regulations such as FTC's "Red Flag" (referenced earlier) rule may address this; additional mitigations may also be necessary. (Booz Allen Hamilton, 2008) For example, consumers with healthcare insurance may be allowing non-insured friends to use their identity to obtain low-cost care.
- Failure of an IT system to retrieve the right data for a patient, presenting data for the wrong patient, allowing undetected changes to data, or not being able to retrieve data due to outages can result in serious medical errors that harm patients. In particular, wireless medical devices and networks – both WiFi and cellular – are vulnerable to outages and low signal strength as well as deliberate denial of service attacks.
- Consumers' privacy-protective behaviors are a significant threat to patients' well-being, as they may withhold relevant clinical data if they believe their privacy is not respected. However, establishing stringent privacy controls ahead of giving treatment to patients, especially in emergent situations, may produce similarly harmful results and medical liability.
- EHRs may be discoverable in civil suits. This raises issues of unanticipated disclosure outside of EHR information of healthcare.

Mitigation Strategies Overview

There are no "silver bullets" to address risks. Rather, it is the combination of the following:

- **Administrative *c*ontrols** – Non-technical controls that ensure the privacy and security policies may be enforced during the course of IT acquisition, implementation, and operation to provide assurances that privacy and security policies and being followed and enforced.

- **Procedural controls** – Documented procedures focused on environmental, physical, and technical controls to ensure privacy and security.
- **Environmental and physical controls** – Privacy and security measures that are either supplied by the environment, such as stable electric power or dependable networks, or implemented as physical controls, such as locked doors or security guard stations.
- **Technical controls** – Portions of an automated system with the purpose of enforcing compliance with privacy and security policies and meeting security objectives.
- **Residual risk controls** – Various non-technical measures to mitigate risks that cannot be effectively or economically handled by other controls, e.g., insurance.

Communication with Stakeholders

For stakeholders to participate in an HIE, it is essential that they trust that privacy will be protected, that information will be appropriately available, and that there will be persistent integrity for all clinically relevant data. For consumers this is informal but analogous to a more formal trust agreement among providers in an HIE.

It is essential that providers and others who are responsible for protecting privacy be forthright about what they are doing and, if breaches occur, report them to the affected parties promptly. Pennsylvania requires such notifications (Pennsylvania General Assembly, 2008), as do other states.

Conforming to Policies and Controlling Risk

Administrative Controls

The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006) identifies several security assurance elements. These are key administrative controls that are followed when acquiring and implementing operating systems that are subject to a set of defined security policies and objectives:

- **Development** – Technical architecture, functional design, structural design, implementation details, security policies, security-relevant features of an IT system.
- **Guidance documents and education** – Preparation for use and secure operation of an IT system and proper handling of privacy-protected healthcare data by employees.
- **Life cycle support** – Life-cycle definition, configuration management scope and capabilities, development security, security tools and techniques, delivery, and security flaw remediation for an IT system.
- **Security Testing** – Coverage, depth, functional tests, and evaluator independence for testing the security functions of an IT system.

- **Vulnerability assessments** – tasks to be done periodically during IT system development and operation to assess system vulnerability, e.g., as part of risk management.
- **Composition** – Rationale, evidence, dependencies, testing, and vulnerability analysis for systems that are composed from multiple IT components.

The Common Criteria also defines discrete levels of assurance for applying these controls. Basically, higher levels of assurance will require greater upfront costs and operating costs. Many systems operate at Level 3 – methodically tested and checked – which is for circumstances in which developers or users require a moderate level of independently assured security via thorough investigation of the system and its development, but without substantial reengineering being required. To assurance healthcare privacy and security protections, Level 4 – methodically designed, tested, and reviewed – may be necessary and further reengineering and retrofitting, at additional cost. Good risk analysis will help determine what level of assurance is required for each circumstance.

Procedural Controls

In the operation of IT systems, manual or automated procedures must be in place to provide management services and system administrators, including:

- Accountability for following and enforcement of privacy and security policies, associating specific identities to those who are accessing IT system resources or data. This includes terminating employees who violate privacy and security policies.
- Privacy disclosure log review, notifications, and alerts to discover instances or patterns of privacy breaches and enable prompt and appropriate actions. This includes making disclosure logs available to consumers upon request.
- Security audit log review, notifications, and alerts to discover instances or patterns of attempted or successful security breaches, including inappropriate access by persons who are authorized to access the data, and to enable prompt and appropriate actions.
- Metrics gathering and reporting to monitor trends and patterns in privacy and security incidents and promote effective administrative actions.
- Processes for making data available, e.g., granting access to authorized persons, importing data from other IT systems, gaining access to data residing on other systems, etc.
- Processes for removing data from shared storage facilities, in particular in response to privacy breaches or consumers' requests. Ongoing public relations programs to communicate with stakeholders regarding ongoing protections, as well as prompt and forthright reporting of privacy violations if they occur.
- Ongoing public relations programs to communicate with stakeholders regarding ongoing protections, as well as prompt and forthright reporting of privacy violations if they occur. Pennsylvania requires such notifications, as do several other states.

The definition of the required procedural controls should be part of the administrative assurance controls defined previously.

Physical and Environmental Controls

In many cases technical security measures exist alongside physical and environmental controls. In some cases they may supply adequate protection, making more sophisticated security technology unnecessary. Risk analysis will help determine those choices.
Physical controls inhibit unauthorized access. Examples of physical controls include:

- Fences
- Locked doors
- Access badges
- Alarms
- Electronic tracking systems, such as RFID tags
- Monitor positioning to hide patient data from unauthorized viewing

Environmental controls are elements in the environment of an IT system that mitigate threats. Examples of environmental controls include:

- Back-up electric generators
- Guard stations
- CCTV cameras and recorders
- Staff training for privacy- and security-protection skills

In the people-intensive environment of healthcare, employee skills are a key environmental control. *Health Information Management and Informatics Core Competencies for Individuals Working with Electronic Health Records* (AHIMA and AMIA, 2008), outlines two sets of necessary employee skills. Ongoing employee education needs to be conducted in the context of procedural controls. The skills are:

- **Privacy and confidentiality of health information skills**
    - Explain legal responsibility, limitations, and implications of actions.
    - Apply the fundamentals of privacy and confidentiality policies and procedures.
    - Follow legal aspects and regulations of documentation in requests for information.
    - Identify legal and regulatory requirements related to the use of personal health information.
    - Identify and apply policies and procedures for access and disclosure of personal health information.
    - Identify policies and procedures regarding release of any patient-specific data to authorized users.
    - Identify what constitutes authorized use of personal health data.
    - Participate in privacy and confidentiality training programs.
    - Follow security and privacy policies and procedures to the use of networks, including intranet and Internet.

- Follow confidentiality and security measures to protect electronic health information.
- Maintain data integrity and validity within an information system.
- Report any possible breaches of confidentiality in accordance with organizational policies.
- Describe the possible consequences of inappropriate use of health data in terms of disciplinary action.
- Describe monetary and prison penalties for breaches.
- Document profession-specific information in an electronic health record.
- Know appropriate methods to correct inaccurate information/errors personally entered in an electronic health record.
- Authenticate information entered in an electronic health record.
- Access reference material available through an electronic health record.
- Identify the source of information entered in an electronic health record.
- Identify, evaluate, select, and appropriately use computer systems for patient information documentation.
- Teach others health record concepts, laws, documentation requirements and organizational policies and procedures as it applies to your work.

- **Health information/data technical security skills**
  - Implement administrative, physical, and technical safeguards.
  - Develop security policies and procedures.
  - Resolve minor technology problems associated with using an electronic health record.
  - Follow access protocols for entry to an electronic health record.
  - Enforce access and security measures to protect electronic health information.
  - Recommend elements that must be included in the design of audit trials and data quality monitoring programs.
  - Implement policies, procedures, and training for health data security.
  - Apply departmental and organizational data and information system security policies.

Technical Controls

Although the HIPAA security rule mentions certain technical controls, it fails to provide a complete and cohesive framework or to define the technical elements needed for effective implementations. Thus, a "HIPAA compliant" system will likely be incomplete and not provide adequate security protections.

The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006) identifies these elements in a way that defines security objectives and evaluates the technology intended to fulfill them:

- **Auditing** – the collection, storage, analysis, and reporting of evidence that the security policies are being enforced and followed, plus evidence of attempts to violate them.

- **Identification and Authentication** – Means for people (or system entities) to identify themselves prior to system access and for systems to obtain assurances that they are, in fact, who they claim to be. It includes rules for the strength of passwords and other authentication data.
- **Data Protection** – Means to grant or withhold permissions for access, ensure intra-system confidentiality, protect integrity, ensure authenticity, enable secure import and export, and inhibit certain accidental disclosures of data. This includes technologies such as e-mail filters and anti-virus protections.
- **Management** – The set of functions to manage all security functions, generally restricted to authorized administrators. This includes user provisioning for identities, passwords, authorizations.
- **Cryptographic support** – The generation, provision, communication, and use of cryptographic technologies to protect data confidentiality and integrity. This especially includes using encryption over the public Internet and protecting wireless networks from snooping by unauthorized people.
- **Nonrepudiation** – Proof that a claimed provider of data did, in fact, send it and it has not been altered. Similarly, proof that an intended recipient of data did, in fact, receive it.
- **Privacy** – Technical means to provide anonymity, pseudonimity, unlinkability, and unobservability of system users and data. The HIPAA privacy rule defines data that must be removed for anonymity when data is reused, e.g., aggregated for research or public health.
- **Protection of the security system itself** – Ensuring that the security system is not a weak point in an otherwise secure system.
- **Resource utilization** – Ensuring that system resources needed to secure operation are available and that there are controls to prevent accidental or deliberate unavailability of system services due to overutilization.
- **System access** – Prevention for multiple access-points for individual users (signed-on at multiple workstations), session and workstation locking when security violations are detected, notification of security policies when user sign-on, and masking passwords when entered.
- **Trusted paths** – The means to establish and maintain secure network connections among system components and with other trusted systems.

CCHIT certification criteria cover only a subset of the above. Those who acquire or build healthcare information systems are responsible for ensuring all technical aspects are in-place and enforcing security policies.

Handling Residual Risk

After all mitigations defined previously have been established, there remains a set of risks that cannot be practically or economically addressed. These residual risks can be mitigated by other means, including:

- **Additional/incremental controls** – monitoring the IT product market and trade journals for new and less expensive security technology, additional training, best practices, etc.
- **Delegation** – enrolling business partners in and HIE or vendors to assume additional risks via trust agreement or business associate agreement amendments. The HIPAA privacy rule requires healthcare providers to have business associate agreements with vendors. Due to the complexities of these, readers should consult an attorney before preparing, negotiating, or signing one.
- **Insurance** – Transferring the financial consequences of risks to an insurance company, essentially pooling risks with other institutions.
- **Seeking additional controls** – monitoring the IT product market and trade journals for new and less expensive security technology, additional training, best practices, etc.
- **Mere acceptance** – Some risks are so unlikely, even if they may have catastrophic consequences, that it is prudent merely to accept them.

Copyright PAeHI, 2009

ENABLING THE SOLUTIONS

Significant value is to be gained by the exchange of health information -- improved quality of care, reduced costs, and improved payment processes.

This white paper supports recommendations from PAeHI, which include:

- Establishing common standards for HIE-related value-added services.
- Defining minimum 'core' and/or value-added service standards.
- Encouraging use of HIE data.
- Establishing 'core' standards related to HIE implementation.
- Accelerating access to pharmacy-related data sources.
- Developing single-standard consolidated data set.
- Ensuring consumer privacy, security and confidentiality are paramount.
- Enabling multi-stakeholder collaboration. .

While the overarching topic of sustainable models for HIE is beyond the scope of this white paper, current proposals always include privacy and security as essential elements (American Health Information Management Association, Foundation of Research and Education, 2008). If providers and consumers do not trust an HIE, they simply will not use it – regardless of how well funded.

Best Practices

Implement the HISPC recommendations (Dimitropoulos, 2007) for common consent forms. They can offer providers assurance that they are complying with Federal and state requirements, and that HIE partners are doing the same.

Implement the HITSP consumer consent specification (Healthcare Information Technology Standards Panel, 2008), a standards-based interoperable means to capture, manage, and communicate rights granted or withheld by a consumer among all HIE partners.

Purchase CCHIT-certified IT products. Privacy and security criteria for CCHIT certification are pragmatically based on IT standards, authoritative sources, and best practices. CCHIT-certified products can be donated to physicians, enabling enable wider use of HIE technologies while avoiding prohibitions in the Stark and Anti-Kickback laws.

View accreditation and certification holistically. Healthcare providers are subject to a variety of accreditation and

> The work being done by HISPC is essential and must lead to federal legislation of a common framework of privacy and security policies for the NHIN, HIEs, and the health care community. Obviously, such a framework will need to allow for scalability of the entity much like HIPAA does today. That, or lead to a framework agreement among the states to effectively do the same.
> *– Don Bechtel, Chief Privacy Officer, HDX, a part of Siemens Health Services, Siemens Healthcare*

certification regimes, e.g., Joint Commission, NCQA, EHNAC, or URAC. They are also subject to privacy and security audits by CMS and other governmental agencies, as well as addressing privacy complaints under HIPAA requirements. Name specific individuals as privacy and security officers charged with ensuring all accreditation, certifications, audits, and violation investigations are consistent.

Use the ISO 27799 standard (International Organization for Standardization, Technical Committee 215, 2006). It defines best practices for healthcare security management and specific guidance for healthcare IT implementation and operation.

The American Medical Informatics Association (AMIA) Open Source Working Group has created a consensus paper on Free/Open Source Software (FOSS). It faults current systems for inadequate safeguards and recommends that software be independently auditable for privacy and security flaws. (American Medical Informatics Association, Open Source Working Group, 2008)

Stakeholder Education

Current arguments in favor of PHRs, EHRs, and HIE lack simple compelling reasons for consumers to risk the privacy of their personal medical histories in the same way that many will trust their credit cards to online vendors.

Informed consumers who trust their privacy will be protected will enable the benefits of an HIE. Healthcare providers are the most convincing source assurance that healthcare information will remain private and secure. The start of the privacy and security value-chain is well-informed healthcare providers who champion the use of trustworthy healthcare information exchange.

Near-term results may be obtained from e-prescribing plus electronic referrals to specialists and clinical laboratories. This will help consumers become experienced and educated about these simplifying technologies.

Education about consents for disclosure is also needed. Finely granular consents, such as unique rules for each caregiver, may leave significant gaps in clinical data. For some consumers, this could be deliberate even if it may cause them medical harm. Educating patients and caregivers to encourage mutual trust can help eliminate the medical risk.

Key Technical Properties

The following are some key system and network properties that are needed to protect privacy and ensure security:

- **Basic Tools** – Basic tooling such as audit repositories and reporting, network encryption, e-mail filters, and anti-virus technology implemented for all user access and server components.

- **Interoperability** – In a privacy and security-protected healthcare IT environment, interoperable systems have trust agreements, shared schemes for identifying users and patients, shared rules for granting and withholding access, and other technical mitigations that ensure sharing of healthcare data with strict confidentiality, availability, and integrity.

- **Scalability** – Systems and networks can accept and new users and additional data without reengineering of the underlying privacy and security protections

- **Usability** – Privacy and security protections operate in a way that does not override, inhibit, distract, or confuse the primary healthcare mission.

- **Affordability** – Privacy and security controls cost less than the total actuarial value of the risks they mitigate.

- **Reasonability** – An HIE-scale solution is inappropriate for smaller providers. HIPAA allows scaling of privacy and security mitigations, not a one-size-fits-all approach.

Demonstration and Model Projects

The Integrating the Healthcare Enterprise (IHE) initiative conducts annual Connectathon events to test the interoperability of healthcare IT products, including security features. In the past three years they have been joined by HITSP, which has published privacy and security specifications. Connectathon's tests are proctored by independent experts.

Vendors whose products have passed Connectathon tests can do live demonstrations at the annual HIMSS conference Interoperability Showcase. This has become the single best-attended exhibit in the HIMSS conference. HITSP has participated in the last two HIMSS Interoperability Showcases and plans to participate in 2009. In 2008, 73 organizations with 51 vendors demonstrated interoperability among 74 different HIT systems. Following the HIMSS conference, subsets of the vendor participants have repeated the demonstration at state and regional events.

> It is not a matter of whether there are barriers that inhibit privacy and security. Rather, the challenge is to develop an HIE in a manner that respects patients' privacy expectations while providing health information that is necessary to improve health care quality and outcomes. – *John P. Houston, vice president, Privacy and Information Security & Assistant Counsel, University of Pittsburgh Medical Center*

Addressing Barriers to Solutions

- **Problems:** Consumers using an HIE may need a separate authorization or consent form for each healthcare provider organization that renders care to them. Patients who receive care at multiple healthcare organizations need multiple forms. Variations in consumer consents for disclosure among healthcare providers leads to inconsistent rules for sharing healthcare information. Administrative and technical solutions are needed to capture/report patient consent

for disclosure status for each organization. Healthcare providers may not be able to afford the changes required for their systems to capture this information and transmit it to an HIE.

Solutions: Define a common set of rules for consent for disclosure within a trusted network, and provide a common registry for them so that consumers can sign once, update them, or withdraw them on-line. Provide a central registry for authorization or consent forms so that consumers can sign once, update them, or withdraw them on-line. Possibly combine this with a Pennsylvania state service such as driver's licenses, Medicaid administration, or income tax returns. This may also require a change in state laws and regulations.

- **Problem:** Lengthy on-line rules and warnings about privacy and security are often overlooked or bypassed, as they get in the way of actually using an IT system. Subsequent complaints about privacy or security violations cannot be answered.

  Solutions: Educate system users before they are allowed access, obtaining affirmative assurance that they understand privacy- and security-relevant aspects. Where technology and healthcare workflow permits, give feedback during system use when a privacy or security relevant policy may be breached.

Copyright PAeHI, 2009

APPENDICES

Definitions

Audit
A record of security-relevant activity within an IT system that serves as evidence that security policies are being enforced and, should violations be attempted, establishes accountability. This is required under the HIPAA security rule and is not the same as the disclosure log required under the HIPAA privacy rule.

Authorization
(1) Process of determining what activities are permitted, usually in the context of authentication.

(2) The permission to perform certain operations or use certain methods or services. (Healthcare Information and Management Systems Society, 2006)

Authentication
The process of proving that a user or system is really who or what it claims to be, protecting against the fraudulent use of a computer system, electronically-stored data, or network resources.

Certification Commission for Healthcare Information Technology (CCHIT)
A recognized certification body (RCB) for electronic health records and their networks, and an independent, voluntary, private-sector initiative. See http://www.cchit.org

Confidentiality
The property the data or information is not made available or disclosed to unauthorized persons or purposes.

Consent for disclosure
Permission granted by an individual for a healthcare provider to use or disclose identifiable health information for treatment, payment, and health care operations purposes **only**. While this is optional under the HIPAA privacy rule, it may be required by state law, and may be combined with consent for treatment unless prohibited by other law.

Covered Entity
From the HIPPA Privacy Rule, a covered entity means: (1) A health plan; (2) A health care clearinghouse; or (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (HIPAA transactions are between health care provider and a health plan or health care clearinghouse.)

Disclosure Log
A mandatory record of all disclosures of healthcare information – with or without consumer consent – that are not for healthcare treatment, payment, operations, or other exempt purposes defined in the HIPAA privacy rule. This includes non-IT events such as written or verbal disclosures. It is not the same as auditing as required by the HIPAA security rule.

Electronic Health Record (EHR)
Electronically stored information about an individual's health history, treatments, and other related information held by a health care provider.

Copyright PAeHI, 2009

Health Information Exchange (HIE)
An infrastructure to enable movement of healthcare information electronically across organizations within a region or community. It must also have agreed-upon business relationships and processes to facilitate information sharing across organizational boundaries

Health Insurance Portability and Accountability Act (HIPAA)
Enacted in 1996, this act requires protection for the confidentiality and integrity of "individually identifiable health information," past, present or future. Privacy and security rules implementing these provisions have been published by The US Department of Health and Human Services.

Healthcare Information Technology Standards Panel (HITSP)
A cooperative partnership between the public and private sectors for the purpose of achieving a widely accepted and useful set of standards specifically to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional and national health information network for the United States. See http://www.hitsp.org

Health Information Security and Privacy Collaboration (HISPC)
A partnership consisting of a multi-disciplinary team of healthcare privacy experts and the National Governor's Association (NGA), HISPC worked with state governments to assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to interoperable health information exchange. *Note: Pennsylvania was not part of HISPC.* See http://www.rti.org/hispc

Individually Identifiable Health Information
A subset of all health information that: (i) is created or received by a health care provider, health plan, employer or health care clearinghouse; (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (iii) contains data that could be reasonably used to identify an individual. The HIPAA privacy rule defines 17 such data elements, but risk analysis may reveal others in particular circumstances.

Interoperability
The ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of healthcare for individuals and communities. (Healthcare Information and Management Systems Society, 2006)

Minimum Necessary
Sharing only the data necessary to accomplish the specific purpose, based on the recipient's need to know as related to the job function's authorizations or legal mandates.

National Health Information Network (NHIN)
Conceptually, a network of disparate health care information systems together to allow consumers, physicians, hospitals, public health agencies, and other authorized users across the nation to share clinical information in real-time under strict security, privacy, and other protections

Personal Health Record (PHR)
Electronically stored information similar to electronic health records but often maintained by an individual and limited to information on the individual's health conditions and treatment history.

Regional Health Information Organization (RHIO)
A neutral organization that adheres to a defined governance structure and like an HIE, facilitates collaboration and coordinates activities to provide the privacy, security, and public trust required to support the exchange of individuals' health information.

Risk
The combination of the probability of an event and its consequences. (Healthcare Information Technology Standards Panel, 2008)

Risk Management
The systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk. (Healthcare Information Technology Standards Panel, 2008)

References

AHIMA and AMIA. (2008). *Health Information Management and Informatics Core Competencies for Individuals Working with Electronic Health Records.*

American Health Information Management Association, Foundation of Research and Education. (2008). Developing a Consensus for Model Health Information Exchange Policies. *NHIN-HISPC-SLHIE Joint Conference.* Dallas, TX: American Health Information Management Association.

American Health Information Management Association, Foundation of Research and Education. (2008). *State-level HIE Value and Sustainability: Approaches for Financing & Bringing Interoperable HIE to Scale (interim report).*

American Medical Informatics Association, Open Source Working Group. (2008). *Free and Open Source Software in Healthcare 1.0.*

Booz Allen Hamilton. (2008). *Medical Identity Theft Environmental Scan.* US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology.

Bordenick, J. C., McGraw, D., Williams, C., Rosati, K. B., & Posnack, S. (2008). Privacy and Confidentiality Issues Critical to Consumers. *eHealth Initiative's Webinar Series.*

Certification Commission for Healthcare Information Technology. (2008). *Certification Commission for Healthcare Information Technology*. Retrieved November 2008, from Certification Commission for Healthcare Information Technology: http://www.cchit.org/

Conn, J. (2008, November 11). Two new Calif. laws add 'teeth' to privacy protection. *Modern Healthcar*e.

Connecting for Health. (2006, October). *The Architecture for Privacy in a Networked Health Information Environment.* Retrieved December 2008, from The Connecting for Health Common Framework: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf

Connecting for Health. (2006). *The Common Framework.* Retrieved November 2008, from Connecting for Health: http://www.connectingforhealth.org

Digital Imaging and Communcation in Medicaine. (2008, October). *CP-895 - Standards for Encrypting Portable Media*. Retrieved November 2008, from DICOM: ftp://medical.nema.org/medical/dicom/cp/cp895_vp.doc

Dimitropoulos, L.,(2007). *Privacy and Security Solutions for Interoperable Health Information Exchange, Final Implementation Plans*. Chicago: Research Triangle Institute.

Golden, J. I. (2008). MN E-Health Initiative and the MN Health Records Act. *PHII Connections Symposium.*

Copyright PAeHI, 2009

Gupta, A. (2008, October 10). *Prescription for Change*. Retrieved November 2008, from Wall Street Journal: http://online.wsj.com/article/SB122426733527345133.html

Halamka, J. (2008, December 1). *Interoperability Advice for the New Administration*. Retrieved December 1, 2008, from Life as a Healthcare CIO: http://geekdoctor.blogspot.com/2008/12/interoperability-advice-for-new.html

Halamka, J. (2008). *Massachusetts Data Protection Regulations*. Retrieved November 2008, from Life as a Healthcare CIO: http://geekdoctor.blogspot.com/

Health Information Trust Alliance. (2008). *Health Information Trust Alliance*. Retrieved November 2008, from Health Information Trust Alliance: http://www.hitrustalliance.org/

Healthcare Information and Management Systems Society. (2006). *HIMSS Dictionary of Healthcare Information Technology Terms, Acronyms, and Organizations.* Chicago: Healthcare Information and Management Systems Society.

Healthcare Information and Management Systems Society. (2008). *HIMSS Security Survey.*

Healthcare Information and Management Systems Society. (2008). *HIMSS09 Annual Conference and Exhibition*. Retrieved December 2008, from HIMSS Interoperabilty Showcase: http://interoperabilityshowcase.org/

Healthcare Information Technology Standards Panel. (2008). *Library of Interoperability Specifications and Constructs*. Retrieved November 2008, from Healthcare Information Technology Standards Panel: http://www.hitsp.org/

Healthcare Information Technology Standards Panel. (2008). *TN 900 - HITSP Security and Privacy Technical Note, version 1.2.* Retrieved November 2008, from Healthcare Information Technology Standards Panel: http://hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=5&PrefixNumeric=900

Healthcare Information Technology Standards Panel. (2008, August). *TP 30 - HITSP Manage Consent Directives Transaction Package.* Retrieved December 2008, from Healthcare Information Technology Standards Panel: http://hitsp.org/Handlers/HitspFileServer.aspx?FileGuid=e067dca7-f011-4798-9bca-99caa6650814

International Organization for Standardization, Technical Committee 215. (2006). *ISO 27799 - Health informatics - Security management in health using ISO/IEC 17799.*

ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation, Version 3.1. (2006). Retrieved November 2008, from The Common Criteria: http://www.commoncriteriaportal.org/theccra.html

Melamedia LLC. (2008). *Health Information Privacy/Security Alert*. Retrieved November 2008, from Melamedia LLC: http://melamedia.com/shopsite_sc/store/html/hipa_intro.html

Minnesota Office of the Revisor of Statutes. (2008). *M.S. §144.293 - Release or disclosure of health records*. Retrieved November 2008, from Minnesota Office of the Revisor of Statutes: https://www.revisor.leg.state.mn.us/statutes/?id=144.293

National Conference of State Legislatures. (2008). *Health Information Technology 2007 and 2008 State Legislation.*

National Conference of State Legislatures. (2008, June). *State Genetic Privacy Laws.* Retrieved December 2008, from National Conference of State Legislatures: http://www.ncsl.org/programs/health/genetics/prt.htm

National Conference of State Legislatures. (2008, November 4). *State Security Breach Notification Laws*. Retrieved November 2008, from National Conference of State Legislatures: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

Patient Privacy Rights Foundation. (n.d.). *Patient Privacy Rights*. Retrieved November 2008, from Patient Privacy Rights: http://www.patientprivacyrights.org

Pennsylvania eHealth Initiative. (2008). *Building a Sustainable Model for Health Information Exchange in Pennsylvania.*

Pennsylvania eHealth Initiative. (2008). *Establishing Widespread Adoption of Electronic Health Records and Electronic Prescribing in Pennsylvania.*

Pennsylvania General Assembly. (2008). *73 P.S. § 2301 - Chapter 43. Breach of Personal Information Notification Act*. Retrieved November 2008, from Unofficial Purdon's Pennsylvania Statutes: http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000

Pritts, J., Choy, A., Emmart, L., & Hustead, J. (2002). *The State of Health Privacy, second edition.* Georgetown University, Health Privacy Project.

Reed Smith LLP. (2003, February). *50 State HIPAA Study*. Retrieved November 2008, from http://www.statehipaastudy.com/

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., & Rogers, G. (2007, December). *SP 800-53 Recommended Security Controls for Federal Information Systems, Revision 2*. Retrieved November 2008, from NIST Computer Security Division, Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

State Alliance for eHealth. (2008). *erating Progress: Using Health Information Technology and Electronic Health Information Exchange to Improve Care.* National Governors Association.

Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). *SP 800-30 Risk Management Guide for Information Technology Systems.* Retrieved November 2008, from NIST Computer Security Division, Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

US Department of Education. (2007, April 27). *Family Educational Rights and Privacy Act (FERPA)*. Retrieved November 2008, from US Department of Eudcation: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

US Department of Health and Human Services and US Department of Education. (2008). *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records.*

US Department of Health and Human Services, Office for Civil Rights. (2008, September 16). *HIPAA*. Retrieved November 2008, from http://www.hhs.gov/ocr/hipaa/

US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Substance Abuse Treatment. (2004). *The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs.*

US Government Accountability Office. (2008). *Health Information Technology - HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains.*

Copyright PAeHI, 2009

US Government Printing Office. (2008, January 1). *16 CFR Part 681 - Federal Trade Commission, Identity Theft Rules.* Retrieved November 2008, from http://www.access.gpo.gov/nara/cfr/waisidx_08/16cfr681_08.html

US Government Printing Office. (2002, October 1). *42 CFR Part 2 - Public Health Service, Department of Health and Human Services, Confidentiality of Alcohol and Drug Abuse Patient Records*. Retrieved November 2008, from http://www.access.gpo.gov/nara/cfr/waisidx_02/42cfr2_02.html

US Government Printing Office. (2008, November 21). *42 CFR Part 3 - Patient Safety and Quality.* Retrieved November 2008, from http://www.access.gpo.gov/nara/cfr/waisidx_02/42cfr2_03.html

US Government Printing Office. (2002, October 1). *45 CFR Parts 160, 162, 164 - HIPAA Privacy and Security Rules*. Retrieved November 2008, from http://www.access.gpo.gov/nara/cfr/waisidx_02/45cfrv1_02.html

Sample Chain of Trust Agreement

Chain of Trust Partner Agreement

This Chain of Trust Agreement is made the __(date)_____, by and between _____ hereinafter referred to as the "HIE" and _____ hereinafter referred to as the "PROVIDER". WHEREAS, PROVIDER performs work which requires it to have access to information regarding HIE'S confidential and protected health information "INFORMATION"; WHEREAS, HIE desires to protect the confidentiality and integrity of the INFORMATION and to prevent inappropriate disclosure of the information; NOW THEREFORE, the parties agree as follows:

BACKGROUND STATEMENTS

A. HIE and PROVIDER are parties to an agreement pursuant to which PROVIDER provides certain services to HIE and, in connection with those services, HIE discloses to PROVIDER certain INFORMATION that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 "HIPAA", Public Law 104-191;

and

B. PROVIDER, as a recipient of INFORMATION from HIE, is a "Business Partner" as that term is defined in HIPAA and regulations promulgated by the U.S. Department of Health and Human Services to implement certain provisions of HIPAA herein "HIPAA Regulations";

and

C. Pursuant to the HIPAA Regulations, all Business Partners of entities such as HIE must, as a condition of doing business with HIE, agree in writing to certain mandatory provisions regarding, among other things, the use and disclosure of INFORMATION;

and

D. The purpose of this agreement is to satisfy the requirements of the HIPAA Regulations, including, but not limited to 45 CFR 164.506(e), as the same may be amended from time to time.

CONFIDENTIALITY

PROVIDER agrees that PROVIDER will not use the INFORMATION in any way detrimental to HIE, and that PROVIDER will keep such INFORMATION confidential. It is understood and agreed by PROVIDER that PROVIDER will notify all applicable business partners and employees of the confidential nature of the INFORMATION and shall direct such parties to treat INFORMATION with due diligence and care. Neither party shall disclose protected health information or other information that is considered, proprietary, sensitive, or confidential unless there is a need to know basis. Both parties agree that they will limit distribution of confidential information to only parties with a legitimate need in performance of the services as herein provided under this Agreement. Disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by the authorized party. This section shall survive the termination, expiration, or cancellation of this Agreement.

TERM

This Agreement shall commence on _____ and the obligations herein shall continue in effect so long as the PROVIDER possesses or has access to any INFORMATION created or received on behalf of HIE. This Agreement will be automatically renewed yearly, unless otherwise terminated by either party. The confidentiality provisions of this Agreement shall survive indefinitely, even beyond the termination of this Agreement.

SAFEGUARDS FOR PROTECTION OF PROTECTED HEALTH INFORMATION

PROVIDER shall implement and maintain, and by this Agreement warrants that it has implemented, such safeguards as are necessary to ensure that INFORMATION disclosed by HIE to PROVIDER is not used or disclosed by PROVIDER except as is provided in this Agreement.

DISCLOSURES REQUIRED BY LAW

In the event that PROVIDER is required by law to disclose INFORMATION, PROVIDER agrees to provide HIE with notice in a timely manner, so that HIE may seek protective order as appropriate.

STATE AND FEDERAL STATUTE COMPLIANCE

PROVIDER warrants and represents that it is in compliance, or will become compliant with all relevant federal/state statutes, rules, regulations and applicable interpretive rulings in a timely manner. Further, both parties agree to remain in compliance with all relevant federal/state statutes, rules, and regulations during the entire term of this Agreement. This includes but is not limited to HRS 323C Privacy of Health Care Information (Act87) and HIPAA. PROVIDER agrees to maintain adequate safeguards to ensure that INFORMATION exchanged between HIE and PROVIDER is protected and used solely for the purposes agreed upon within this Agreement. Failure to comply with this provision can result in immediate and automatic termination of previously agreed upon business relationship, without penalty or cost to either party.

POLICY AND PROCEDURE REVIEW

PROVIDER shall make available on demand to HIE a copy of all Policies and Procedures relevant to safeguarding INFORMATION.

REPORT OF IMPROPER DISCLOSURE OR SYSTEMS COMPROMISE

HIE and PROVIDER agree to immediately notify all parties within their "Chain of Trust" of any improper or unauthorized access and disclosure of the INFORMATION, any misuse of the INFORMATION, including but not limited to systems' compromises. HIE and PROVIDER will take all necessary steps to prevent and limit any further improper or unauthorized disclosure and misuse of information. PROVIDER shall also maintain an incident log of all improper or unauthorized disclosures. At the request of HIE, PROVIDER will make available to HIE a copy of incident log.

RETURN OF MATERIALS

Unless otherwise specifically required by statute or rule, PROVIDER shall promptly return to HIE all material containing or reflecting any HIE proprietary information whether prepared by HIE or as a result of providing services for which the PROVIDER has been specifically authorized by HIE. In addition, the PROVIDER shall exercise due diligence to destroying the INFORMATION in a manner that will render non-identifiable all documents, memoranda, notes or other writings prepared by PROVIDER, or its representatives, which are based on the INFORMATION

SUB-CONTRACTORS:

If PROVIDER discloses INFORMATION to any subcontractor, independent contractor, or agent, it shall require such party to execute a Chain of Trust Agreement that upholds the standards contained within this Agreement.

GOVERNMENT ACCESS TO RECORDS

In Accordance with 42 U.S.C. section 1395x(v)(1)(I), PROVIDER agrees that until the expiration of six (6) years after the completion of services pursuant to this Agreement, PROVIDER shall make available, upon written request to the Secretary of Health and Human Services, (for Comptroller General of the United States or any of their duly authorized representatives) its contract and books, its documents, and records which are necessary to certify the nature and extent of the cost for services agreed herein to be provided. Further, if PROVIDER carries out its duties hereunder through a subcontract with a value or cost of $10,000.00 or more over a twelve-month period, such subcontractor shall make available, until the expiration of six (6) years after completion of services pursuant to this Agreement, upon written request to the Secretary of Health and Human Services, (for Comptroller General of the United States, or any of their duly authorized representatives) its subcontract, books, documents, and records which are necessary to certify the nature and extent of the cost for the services agreed herein to be provided.

ADDITIONAL ACCESS TO INFORMATION

If PROVIDER significantly alters the INFORMATION provided by, HIE shall have the right to access the altered information upon written request to PROVIDER. Such access shall be provided to HIE within a reasonable period

after receipt of the request and shall be during the normal business hours of PROVIDER. PROVIDER shall incorporate changes or amendments to the INFORMATION if requested by the HIE.

INJUNCTIVE RELIEF

PROVIDER acknowledges that the remedy at law for any breach by it or the terms of this Agreement shall be inadequate and that the damages resulting from such breach are not readily susceptible to being measured in monetary terms. Accordingly, in the event of a breach or threatened breach by PROVIDER of the terms of this Agreement, HIE shall be entitled to immediate injunctive relief and may obtain a temporary order restraining any threatened or further breach. Nothing herein shall be construed as prohibiting HIE from pursuing any other remedies available to HIE for such breach or threatened breach, including recovery of damages from PROVIDER. PROVIDER further represents that it understands and agrees that the provisions of this agreement shall be strictly enforced and construed against it.

THIRD PARTY BENEFICIARIES

Both parties understand and agree that other parties (individuals or entities) who are the subject of the INFORMATION provided to PROVIDER are intended to be third party beneficiaries of this Agreement.

SEVERABILITY

In the event that any provision of this Agreement violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

CONSTRUCTION OF AGREEMENT

The language in all parts of this Agreement shall in all cases be simply construed according to its fair meaning and not strictly for or against the PROVIDER or HIE. The headings preceding each paragraph are for convenience only and shall not in any way be construed to affect the meaning of the paragraphs themselves.

HOLD HARMLESS

PROVIDER agrees to indemnify, defend and hold harmless HIE, its directors, officers, agents, shareholders, and employees against all claims, demands, or causes of action that may arise from PROVIDER'S employees, agents, or independent contractors improper disclosure of the INFORMATION and from any intentional or negligent acts or omissions.

ENTIRE AGREEMENT; AMENDMENTS; NO WAIVER

This Agreement contains the entire agreement between the parties with respect to the matters covered by this Agreement and supersedes all prior negotiations, agreements and employment contracts between the parties, whether oral or in writing. This Agreement may not be amended, altered or modified except by written agreement signed by all parties of this Agreement. No provision of this agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

AUTHORITY

The persons signing below have the right and authority to execute this Agreement for their respective entities and no further approvals are necessary to create a binding Agreement.

GOVERNING LAW

This Agreement shall be governed by the laws of the State of Pennsylvania and shall be construed in accordance therewith. IN WITNESS WHEREOF, the parties have executed this CHAIN OF TRUST AGREEMENT the day and year first written above.

Signatures of the parties follow

Sample Patient Consent Forms

Practice Name
Address and Phone Number
HIPAA PATIENT CONSENT FORM

Our Notice of Privacy Practices provides information about how we may use and disclose protected health information about you. The Notice also contains a patient rights section describing your patient rights under the law. You have a right to review this notice before signing the consent. The terms of the notice may change, and if this should occur, you may receive a revised copy by contacting the office.

You have the right to restrict how protected health information about you is used or disclosed for treatment, payment, or healthcare operations. We are not required to agree to this restriction, but if we do, we shall honor that agreement.

By signing this form, you consent to our use and disclosure of protected health information about you for treatment, payment, or healthcare operations. You have a right to revoke this consent in writing, signed by you. However, such a revocation shall not affect any disclosures we have already made in relation to you on your prior consent. The practice provides this form to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The patient understands that:

1) Protected health information may be disclosed or used for treatment, payment, or health care operations.
2) The practice has a Notice of Privacy Practices and the patient has the opportunity to review this notice.
3) The practice reserves the right to change the notice of privacy practices.
4) The patient has the right to request restricted use of their information, but the practice does not have to agree to those restrictions.
5) The patient may revoke this consent in writing at any time and all future disclosures will then cease.

The Consent is signed by:

Printed Name (Patient name or representative)

Signature & Date

Copyright PAeHI, 2009

Universal Authorization for the Release of Medical Information
[Full Organization Name]
[Organization Address]

[Org Name] understands your medical care may be managed by both [Org Name] and non-[Org Name] healthcare teams. Your doctors believe that having a complete picture of your health status is important to providing quality medical care. This can be especially important in the case of an emergency room visit.

Your [Org Name][1] healthcare team uses 'Computer Systems'[2] and paper documents to record care provided at a [Org Name] office or hospital. We need your approval to share your [Org Name] medical information with non-[Org Name] healthcare teams involved in your medical care. We ask that you review and sign this authorization.

Here are the key points we want you to understand:

- By initialing and signing this authorization, you are giving us permission to release your medical information to non-[Org Name] licensed healthcare teams who are involved in your care.
- This authorization covers the complete release of your medical information, current and future, and includes information on alcoholism, drug abuse, mental health, and HIV/AIDS if any apply to you.
- Protecting your medical information is very important to us. Security measures are in place to protect the privacy and confidentiality of your medical information.
- Non-[Org Name] healthcare teams, who have access to the Computer Systems, will be able to view, print and retain your medical information. Therefore medical information may be further released by your non-[Org Name] healthcare team and may no longer be protected by federal privacy regulations (HIPAA).
- This authorization will be in effect until you revoke or cancel it as described in our Notice of Privacy Practices. To revoke an authorization, please submit a written request at your next doctor's visit or send it to the address at the top of this page. We are not able to take back any uses or disclosures already made with your authorization.
- If you choose to not sign this authorization, treatment or payment services provided to you by [Org Name] will not be affected. Concerns or questions about this authorization? You can call [1-888-555-5555] and ask for '[contact]'.

I hereby authorize [Org Name] to release my medical information to non-[Org Name] licensed medical providers and their approved staff who are involved in my care for the purpose of my medical evaluation or treatment. This includes my medical information stored in Computer Systems and paper documents.

Patient Initials	Parent/Guardian Initials	By initialing these 3 items, I acknowledge that information regarding these topics may be released as part of my medical information
		Alcoholism or drug abuse or drug dependency - evaluation, diagnosis and/or treatment
		Mental health/rehabilitation or neuro-psychological issues - evaluation, diagnosis and/or treatment
		HIV/AIDS - evaluation, diagnosis and/or treatment

Patient, age 14 and older, please date & sign here and initial all 3 items in the box above.

Date: _____ Patient Signature: _____

If patient is a minor under age 18 (unemancipated) or if patient is unable to give consent, parent or legal guardian must also complete the following and initial all 3 items in the box above.

Date: _____ Parent/Legal Guardian Signature: _____

Relationship to Patient: _____

1 [Org Name] is comprised of [List corporate entities if applicable].

2 'Computer Systems' include applications used to electronically store clinical patient data [excluding…(if applicable)].

*** A copy of completed authorization form must be given to patient. ***

Copyright PAeHI, 2009

Sample Business Associate Agreements

The following is a sample business associate agreement for Pennsylvania healthcare providers, provided as an illustration. Please do not use it verbatim. It is very important to consult with an attorney before establishing such an agreement.

BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the "Business Associate Agreement") entered into by and between Vendor Company, with its principal office at _____ ("Vendor") and Provider ("Customer"), a Pennsylvania not-for-profit corporation located _____ , (collectively, the "Parties") is effective as of _____, 2008 (the "Agreement Effective Date")

WHEREAS, the Parties have executed an agreement or agreements under which Vendor provides certain products or services to Customer including, but not limited to, any amendments, contract supplements or product requisitions referencing any agreement(s) (singly, the "Agreement" and collectively the "Agreements").

WHEREAS, HIPAA, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the federal HIPAA privacy and security regulations promulgated pursuant thereto and codified at 45 C.F.R. parts 160 and 164 (the "Privacy Rule") and 45 C.F.R. parts 160, 162, and 164 (the "Security Rule") (collectively referred to as the "HIPAA Regulations"), may require certain entities covered by the HIPAA Regulations to place certain provisions in their agreements with third parties who come into contact with certain patient health information;

WHEREAS, the Parties have determined that it is in their respective interests to comply with said rules and now desire to amend the Agreement(s) as of the Business Associate Agreement Effective Date on the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the mutual exchange of promises set forth herein, Vendor and Customer agree to the following terms:

Except as defined herein or otherwise required by the context herein, all capitalized terms used in this Business Associate Agreement have the meaning set forth in the Agreement(s). Any provisions in the Agreement(s) relating to the confidentiality of information are hereby stricken and replaced with the following:

1. CONFIDENTIALITY.

   a. Confidential Information. Each party (the "Discloser") may disclose to the other party (the "Recipient") certain non-public information relating to the Discloser's business, including, but not limited to, technical, marketing, financial, personnel, planning, medical records and other information that is marked confidential, which the Recipient should reasonably know to be confidential given the nature of the information and the circumstance of disclosure, and/or that derives independent value from not being generally known to the public ("Confidential Information"). Confidential Information of each party shall also include the terms of this Agreement, but not the existence and general nature of this Agreement. Confidential Information will not include any information:

      i. lawfully obtained or created by the Recipient independently of, and without use of, Discloser's Confidential Information and without breach of any obligation of confidence; or

      ii. that is in or enters the public domain without breach of any obligation of confidence.

   b. Use and Disclosure. Except as expressly permitted by this Agreement, the Recipient will:

      i. not disclose, transfer, dispose of, reproduce, or make Discloser's Confidential Information available to any third party, directly or indirectly, except with the prior consent of the Discloser and except (i) to the employees or contractors of the Recipient to the extent that they need to know that Confidential Information for the purpose of performing the Recipient's obligations under this Agreement in accordance with its terms, and who are bound by confidentiality terms with respect to that Confidential Information no less restrictive than those contained in this Agreement; or (ii) as required to be

disclosed by law, to the extent required to comply with that legal obligation, provided that the Recipient will promptly notify the Discloser of such obligation in such a manner that allows the Discloser a reasonable opportunity to secure the protection of such Confidential Information;

ii. use the Discloser's Confidential Information only for the purpose of performing Recipient's obligations under this Agreement; and

iii. use all reasonable care in handling and securing the Discloser's Confidential Information, and employ all reasonable data security measures that the Recipient ordinarily uses with respect to its own proprietary information of similar nature and importance, which shall in no event be less than a commercially reasonable degree of care and security.

c. Return of Confidential Information. The Recipient will return to the Discloser, and destroy or erase all of the Discloser's Confidential Information in tangible form, upon the expiration or termination of this Agreement, and the Recipient will promptly certify in writing to the Discloser that it has done so.

2. HIPAA BUSINESS ASSOCIATE OBLIGATIONS.

Definitions

"Compliance Date" refers to the date upon which Customer is required to be in compliance with the applicable HIPAA Regulation.

"Designated Record Set" means a group of records maintained by or for Customer that are the medical records and/or billing records of individual patients or are otherwise used by Customer to make decisions about individual patients.

"Individually Identifiable Health Information" means individually identifiable health information as defined at 45 C.F.R. § 160.103.

"Protected Health Information" or "PHI" means Individually Identifiable Health Information (transmitted or maintained in any form or medium) received from, or created or received by Vendor on behalf of, Customer and concerning Customer patients or the patients of any of Customer's health care provider Customers.

All capitalized terms used herein that are not otherwise defined have the meanings ascribed in the HIPAA Regulations.

3. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PROTECTED HEALTH INFORMATION.

- Responsibilities of Vendor. With regard to PHI, as of the Compliance Date set forth under the applicable HIPAA Regulation, Vendor agrees as follows:

1. Vendor will use and/or disclose the PHI only as permitted or required by this Agreement, in accordance with its terms, or as required by law; and will comply with all other relevant sections of the HIPAA Regulations as the same may be amended from time to time.

2. Vendor will not use, disclose or transmit PHI for re-disclosure in any manner that would violate the requirements of the HIPAA Regulations.

3. At all times during this Agreement, Vendor's use and disclosure of PHI is subject to the minimum necessary standards set forth in the HIPAA Regulations. Vendor will only use and disclose the PHI that is minimally necessary to perform its obligations under this Agreement or as required by law.

4. Vendor will implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy and security of PHI including, but not limited to, safeguards necessary to ensure that: (i) PHI is not used or disclosed by Vendor except as is permitted or required in this Agreement or under the law; (ii) access to PHI is limited to authorized personnel of Vendor; (iii) Vendor's security systems and procedures meet the highest professional industry standard to protect PHI; and (iv) the confidentiality, integrity and availability of PHI is protected in accordance with the standards and implementation specifications set forth under the Security Rule. Vendor shall promptly notify Customer of any material change to any aspect of its privacy and security safeguards.

5. Vendor will not transmit PHI over the Internet or any other insecure or open communication channel unless such information is encrypted using encryption standards generally accepted in the health care community and in compliance with the HIPAA Regulations, unless otherwise agreed to by the parties. If Vendor stores or maintains PHI in encrypted form, Vendor will, promptly at Customer's request, provide Customer with the key or keys to decrypt such information.
6. Vendor will immediately report to Customer any use or disclosure of PHI of which Vendor becomes aware that is not permitted by this Agreement (including, but not limited to any Security Incidents).
7. Vendor will mitigate, to the extent practicable, any harmful effect known to Vendor that is the result of, or arises from, Vendor's unauthorized use or disclosure of PHI.
8. To the extent Vendor is permitted to utilize an agent or subcontractor to perform any of its obligations under this Agreement, Vendor will require all such subcontractors and agents that receive or use, or have access to, PHI under the Agreement to agree, in writing, to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Vendor pursuant to this Agreement.
9. Upon request, Vendor will immediately make available its internal practices, books and records relating to the use and disclosure of PHI to the Secretary of HHS, or the Secretary's designee, for purposes of determining Customer's compliance with applicable HIPAA Regulations, and upon reasonable notice, shall afford Customer the right and opportunity to review Vendor's records relating to Vendor's use and disclosure of PHI.
10. Vendor will provide to Customer such information in Vendor's possession as is reasonably requested by Customer and necessary to enable Customer to respond to a request by an individual for an accounting of the disclosures of the individual's PHI in accordance with HIPAA.
11. Unless otherwise explicitly stated in an applicable Contract Supplement, the parties do not intend for Vendor to maintain any PHI in a Designated Record Set for Customer. If Vendor maintains any PHI in a Designated Record Set, then Vendor agrees to (1) provide such PHI to Customer in the time and manner requested by Customer in writing, and (2) to make amendments to such PHI in accordance with the Privacy Rule.
12. If Vendor believes it has a legal obligation to disclose any PHI, it will notify Customer as soon as reasonably practical after it learns of such obligation, and in any event within a time sufficiently in advance of the proposed release date such that Customer's rights would not be prejudiced, as to the legal requirement pursuant to which it believes the PHI must be released. If Customer objects to the release of such PHI, Vendor will allow Customer to exercise any legal rights or remedies Vendor might have to object to the release of the PHI, and Vendor agrees to provide such assistance to Customer, at Customer's expense, as Customer may reasonably request in connection therewith.

- Software Maintenance. Vendor warrants and represents that the software (as it functions alone or in combination with any required hardware and/or third-party software) licensed by Customer pursuant to this Agreement, if any, (the "Software") is and will remain, in full compliance with all applicable federal and state requirements and regulations (including HIPAA and other laws or regulations related, in whole or in part, to confidentiality or privacy). Vendor shall modify the Software as necessary to conform to changes in any such laws or regulations, free of charge to Customer so long as Customer continues to subscribe to Vendor's support and/or maintenance services. Vendor understands that time is of the essence, and will use its best efforts to achieve technically and commercially viable modifications or enhancements in a timely manner.
- Responsibilities of Customer. Customer agrees to obtain any consent or authorization that may be required by HIPAA, or applicable state law, prior to furnishing Vendor with PHI. Customer agrees to timely notify Vendor, in writing, of any arrangements between Customer and the individual that is the subject of PHI that may impact in any manner the use and/or disclosure of that PHI by Vendor under this Agreement.

4. EFFECT OF REGULATORY CHANGES ON RESPONSIBILITIES OF THE PARTIES.

- The Parties agree to amend or modify this Agreement as necessary, to comply with any applicable regulatory revisions or to better serve the Parties' business practices.
- To the extent that any relevant provision of HIPAA or other applicable law concerning the privacy or security of PHI is enacted or materially amended in a manner that changes the obligations of Customer or Vendor that are embodied in term(s) of this Agreement, the Parties agree to negotiate in good faith and take such action as necessary to bring performance under this Agreement into compliance with the HIPAA Regulations or other applicable law, including without limitation, amending or modifying this Agreement and/or, to the extent applicable, updating or otherwise modifying the Software. If, after negotiating in good faith, the parties are unable to mutually agree on an appropriate compliance methodology or approach, Customer may unilaterally terminate this Agreement, if it determines in good faith that such course of action is the only reasonable approach under the circumstances to enable Customer to comply with the HIPAA Regulations or other applicable law.
- All amendments to this Agreement shall be in writing and signed by the party against whom enforcement is sought.

5. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION.

- Permitted Uses and Disclosures of PHI by Vendor. Except as specified below, Vendor may only access, duplicate or otherwise use or disclose PHI as necessary to perform its obligations under the Agreement, provided that such use or disclosure would not violate HIPAA if done by Customer. All other uses or disclosures not authorized by this Agreement are prohibited. Unless otherwise permitted by this Agreement, Vendor will not permit the disclosure of any PHI to any person or entity other than such of its employees, agents or subcontractors who must have access to the PHI in order for Vendor to perform its obligations under this Agreement and who agree to keep such PHI confidential as required by this Agreement. Unless otherwise limited herein, Vendor may:
  1. use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of Vendor.
  2. disclose the PHI in its possession to a third party for the purpose of Vendor's proper management and administration or to fulfill any legal responsibilities of Vendor, provided that (i) the disclosures are required by law, or (ii) Vendor has received from the third party reasonable assurances regarding the confidential handling of such PHI as required under HIPAA (including, but not limited to, assurances such PHI will be held confidentially and only used or further disclosed as required by law or for the purpose for which it was disclosed to such third party).
  3. aggregate the PHI obtained by Vendor as a business associate, provided that Customer has authorized the aggregation and the purpose of such aggregation is to provide Customer with data analyses relating to the Health Care Operations of Customer.
- Ownership of PHI. As between Customer and Vendor, Customer holds all right, title and interest in and to the PHI, and Vendor does not hold, and will not acquire by virtue of this Agreement or by virtue of providing any services or goods to Customer, any right, title or interest in or to the PHI or any portion thereof. Except as specified in paragraph (c) above or as otherwise agreed to in writing by the parties, Vendor will have no right to compile and/or distribute statistical analyses and reports utilizing aggregated data derived from the PHI or any other health and medical data obtained from Customer.

6. TERM & TERMINATION OF AGREEMENT.

- Term. This Business Associate Agreement shall remain in effect for so long as Vendor continues to maintain PHI or perform in its capacity as a Business Associate to Customer.
- Termination by Customer. Customer may immediately terminate the Agreement if it determines that Vendor has violated a material term of this Business Associate Agreement or any other applicable privacy or confidentiality laws or regulations. Alternatively, Customer may provide Vendor with prompt written notice of an alleged material breach and afford Vendor an opportunity to cure the alleged breach. Failure to cure the material breach within thirty (30) days of receipt of notice is grounds for the immediate termination of this Agreement.

cure the material breach within thirty (30) days of receipt of notice is grounds for the immediate termination of this Agreement.

- Alternative to Termination. In the event that Customer elects to continue this Agreement in full force notwithstanding Vendor's material breach, Customer may require Vendor to: (a) exercise all reasonable efforts to retrieve any improperly used or disclosed PHI; (b) establish and adopt additional reasonable practices, policies and/or procedures to assure that PHI is not used or disclosed in violation of this Agreement; (c) comply with all reasonable requests by Customer to demonstrate Vendor' future compliance with the Agreement; and/or (d) take such other actions as Customer may reasonably request.
- Return of PHI. Upon the expiration or termination of this Agreement, for any reason, Vendor will promptly return to Customer, or at Customer's sole option destroy, any PHI in the possession or control of Vendor or any agent or subcontractor of Vendor, retain no copies of such PHI, and provide Customer with certification of such return or destruction, and, unless otherwise expressly agreed to in writing, any right or license which Vendor has to use the PHI will terminate immediately upon such expiration or termination of the Agreement. If Customer determines that the destruction or return of the PHI is not reasonably feasible, the protections contained in this Agreement will continue to apply to any retained PHI, and any further use or disclosure of such PHI by Vendor, its agents or subcontractors, is limited solely to those purposes that made the return or destruction of such PHI infeasible.

7. RIGHT TO INJUNCTIVE RELIEF.

   Vendor expressly acknowledges and agrees that the breach, or threatened breach, by it of any provision of this Business Associate Agreement may cause Customer to be irreparably harmed and that Customer may not have an adequate remedy at law. Therefore, Vendor agrees that upon such breach, or threatened breach, Customer will be entitled to seek injunctive relief to prevent Vendor from commencing or continuing any action constituting such breach without having to post a bond or other security and without having to prove the inadequacy of any other available remedies. Nothing in this paragraph will be deemed to limit or abridge any other remedy available to Customer at law or in equity.

8. INDEMNIFICATION.

   Vendor shall indemnify, defend and hold harmless Customer and its affiliates, officers, directors, employees, and agents (the "Indemnified Party or Parties") from and against any and all actual and threatened losses, liabilities, damages, claims and all related costs and expenses (including reasonable legal fees and costs of litigation, settlement, judgment, interest, fines and penalties) ("Losses") arising from or in connection with the acts or omissions of Vendor's employees, agents or contractors in connection with this Business Associate Agreement, including, without limitation, Losses sustained by third parties that may at any time be incurred by Customer to the extent based upon allegations that Vendor materially breached any of the terms and conditions of this Business Associate Agreement. Customer shall cooperate with Vendor, at Vendor's expense, in defending or settling such claim and the Indemnified Party may participate in the defense of any such claim through counsel of its choice at its own expense. Vendor will defend at its expense, any action brought against the Indemnified Party related to any matter covered by the indemnification hereinbefore provided, and will pay any costs (including reasonable attorneys' fees) and damages incurred by or finally awarded against the Indemnified Party in such action or constituting a settlement of such claim.

9. NO THIRD PARTY BENEFICIARIES.

   Vendor may not assign this Business Associate Agreement without the prior written consent of Customer. Nothing in this Business Associate Agreement shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

10. CONFLICTS.

    Except as otherwise modified by this Business Associate Agreement, all other terms and conditions of the Agreement(s) shall remain in full force and effect; however, in the event of a conflict between the terms of the Agreement(s) and this Business Associate Agreement, the terms of this Business Associate Agreement shall control.

11. COMPLIANCE CERTIFICATION.

The authorized representative of Vendor, whose signature appears below, hereby certifies and warrants that Vendor is presently in compliance with the terms of this Business Associate Agreement and that Vendor shall maintain its compliance with all applicable HIPAA requirements for the duration of the obligation giving rise to this Business Associate Agreement.

IN WITNESS WHEREOF, the Parties have caused this Business Associate Agreement to be executed by their duly authorized representatives.

Signatures of the parties follow

The following is a business associate addendum for a physician group practice, provided as an illustration. Please do not use it verbatim. It is very important to consult with an attorney before establishing such an agreement.

[Practice Name]

Business Associate Addendum

I.General

A.Effective Date

The effective date of this addendum is _____.

B.Parties

The parties to this addendum are (Practice Name) ("Covered Entity"), a physician group practice with its principal office at _____ and _____ ("Business Associate"), a with its principal office at _____ (collectively, the "Parties").

C.Purpose of Addendum

Covered Entity is subject to the following rules promulgated by the Department of Health and Human Services ("DHHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"):

- Privacy Rule (a/k/a/ Standards for Privacy of Individually-Identifiable Health Information) – This rule is published at 45 C.F.R. Part 164. It establishes standards for the privacy of personal health information. Covered Entity is required under the rule to obtain privacy assurances from certain entities to which it discloses health information protected by the rule ("Protected Health Information") and/or which it allows to create or receive Protected Health Information on its behalf.
- Transactions and Code Sets Rule – This rule is published at 45 C.F.R. Part 162. It establishes standards for electronic submission of claims and other health care transactions ("Transactions"). Covered Entity is required under the rule to require certain entities which conduct Transactions in whole or part on its behalf to comply with the rule with respect to such Transactions and to require their agents and subcontractors to comply with the rule with respect to such Transactions.

    - On _____, the parties entered into an agreement ("Core Services Agreement") providing for Business Associate to provide _____ Services to Covered Entity. Business Associate will regularly receive and/or create Protected Health Information in the course of performing these services and other duties and responsibilities under the Core Services Agreement. The Core Services Agreement also provides for Business Associate to conduct Transactions on behalf of Covered Entity. The purpose of this Addendum is to incorporate those terms and conditions required by the Privacy Rule and the Transactions and Code Sets Rule.

    [References to Transactions and Code Sets Rule provisions may be removed if not applicable.]

D.Legally bound

The Parties agree to be legally bound to the terms and conditions set forth in this Addendum. The Addendum is incorporated into and shall be deemed to be part of the Core Services Agreement.

II.Definitions

A.Defined terms

"Core Services Agreement" shall mean the agreement entered into by the parties on_____ provided for Business Associate to deliver _____ services to Covered Entity.

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

"Other state and federal privacy laws" include, but are not limited to professional licensing regulations for physicians (49 Pa. Code §16.61, §25.213), the Confidentiality of HIV-Related Information Act (35 P.S. §§7601-7612), the Mental Health Procedures Act and regulations (50 P.S. §7111; 55 Pa. Code §5100.31-5100.39), and the federal protections for drug and alcohol abuse treatment records (42 C.F.R. §§2.1-2.67).

"Privacy Rule" shall mean the Standards for Privacy of Individually-Identifiable Health Information promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act at C.F.R. Part 160 and Part 164, Subparts A and E.

"Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. §164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

"Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. §164.501.

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

"Transaction" means a transaction subject to the Transaction and Code Set Rule.

"Transactions and Code Set Rule" shall mean the Transactions and Code Set rule promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act at 45 C.F.R. Parts 160 and 162.

B.Other definitions

Any other term used, but not otherwise defined, in this Addendum shall have the same meaning as given the term in 45 C.F.R. §§160.103 & 164.501.

III.Permitted uses and disclosures by Business Associate

A.General uses and disclosures

Except as otherwise limited in this Addendum, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Core Services Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of Covered Entity.

B.Specific uses and disclosures

1.Management and Administrative Uses

Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information in accordance with 45 C.F.R. §164.504 (e)(4)(i) for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. [This provision is only necessary if the physician practice desires to allow the Business Associate to use PHI for its management and administration purposes.]

2.Management and Administration Disclosures

Except as otherwise limited in this Addendum, Business Associate may disclose Protected Health Information to third parties in accordance with 45 C.F.R. §164.504 (e)(4)(ii) for the proper management and administration of the Business Associate, provided that (i) the disclosures are Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. [This provision is only necessary if the physician practice desires to allow the Business Associate to disclose PHI for its management and administrative purposes.]

3.Data Aggregation Services

Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. §164.504(e)(2)(i)(B). [This provision is only necessary if the physician practice desires to allow the Business Associate to use and disclose PHI for data aggregation purposes.]

4.Reporting Violations of Law

Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. §164.502(j)(l). [This provision is optional.]

IV.Obligations and Activities of Business Associate

A.Prohibited uses and disclosures

Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Addendum or as Required By Law.

B.Safeguards

Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Addendum.

C.Mitigation

Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Addendum. [This provision is not mandated. The model language states that is may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages by a Business Associate.]

D.Self-Reporting

Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Addendum of which it becomes aware. The report shall be in writing and made within _____ days of Business Associate's discovery of the unauthorized use and/or disclosure. [The requirement that the report be in writing and within a specified time-period is not mandated.]

E.Agents and Subcontractors

Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees in writing to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information. [The requirement that the assurances be written is not mandated.]

F.Access to Protected Health Information

Business Associate agrees to provide access, at the request of the Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set (as defined by Covered Entity), to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R.

§164.524. [Negotiated time and manner terms that are consistent with the privacy rule may be included in lieu of the language leaving those matters to the discretion of the Covered Entity. This provision is not necessary if the business associate does not have protected health information in a designated record set.]

G.Amendments to Protected Health Information

Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity. [Negotiated time and manner terms that are consistent with the privacy rule may be included in lieu of the language leaving those matters to the discretion of the Covered Entity. This provision is not necessary if the business associate does not have protected health information in a designated record set.]

H.Cooperation with Audits and Investigations

Business Associate agrees to make internal practices, books and records, including policies and procedures and Protected Health Information, related to use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to Covered Entity or to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. [In the case of disclosures to the Covered Entity, negotiated time and manner terms that are consistent with the privacy rule may be included in lieu of the language leaving those matters to the discretion of the Covered Entity.]

I.Other Compliance Cooperation

Business Associate agrees to make internal practices, books and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, in a time and manner designated by the Covered Entity, for purposes of Covered Entity determining Business Associate's compliance with this Addendum. [Negotiated time and manner terms that are consistent with the privacy rule may be included in lieu of the language leaving those matters to the discretion of the Covered Entity. This provision is not mandatory.]

J.Documentation of Disclosures

Business Associate agrees to document such disclosures of Protected Health Information and information related to

such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.

K. Accounting of Disclosures

Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designed by Covered Entity, information collected in accordance with Section IV.J. of this Addendum, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528. [Negotiated terms regarding the time and manner of the provision of information may be included in lieu of the language leaving those matters to the discretion of the Covered Entity.]

L. Other state and federal privacy laws

Notwithstanding any other provision in this Addendum, Business Associate shall comply with other state and federal privacy laws (except to the extent that they are pre-empted by the Privacy Rule) and shall not engage in any activity that would result in Covered Entity being in violation of any other state or federal privacy law. [This provision is not mandatory.]

M. Compliance with Transactions and Code Sets Rule

If Business Associate conducts a Transaction in whole or part for or on behalf of Covered Entity, Business Associate shall comply with all applicable requirements of the Transactions and Code Sets Rule and require any agent or subcontractor to comply with all applicable requirements of the Transactions and Code Sets Rule.

V. Obligations of Covered Entity

A. Notice of Privacy Practices

Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. §164.520, to the extent that the limitation may affect Business Associate's use or disclosure of Protected Health Information.

B. Status of Individual Permissions

Covered Entity shall provide Business Associate with any change(s) in, revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that the change may affect Business Associate's permitted or required uses and disclosures.

C. Restrictions on Use and Disclosure

Covered Entity shall notify Business Associate of any restriction(s) to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that the restriction may affect Business Associate's permitted or required uses and disclosures.

D. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except for data aggregation or management and administrative activities of the Business Associate that are authorized under Section III.B of this Addendum.

VI. Term and Termination

A. Term

The Term of this Addendum shall be effective as of _____, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section VI.

B. Automatic termination

This Addendum shall automatically terminate without any further action of the Parties upon the termination or expiration of the Core Services Agreement. In the event of such a termination, the provisions of Section VI.D shall apply.

C.Termination for Cause

1.Material Breach

In the event that Covered Entity determines that Business Associate has materially breached this Addendum, Covered Entity may either, in its sole discretion, (i) immediately terminate this Addendum, the Core Services Agreement and any other related agreements, (ii) provide Business Associate with an opportunity to cure the breach in accordance with Section VI.C.2, or (iii) report the violation to the Secretary. In the event of a termination pursuant to this section, the action of the Secretary, or otherwise, the provisions of Section VI.D shall apply.

2.Opportunity to cure option

Covered Entity may elect to notify Business Associate of a material breach and provide Business Associate with the opportunity to cure the breach upon mutually satisfactory terms. Provided however, in the event that the Parties do not agree to mutually satisfactory terms within _____ days, Business Associate shall cure the breach to the satisfaction of the Covered Entity within _____ days. Business Associate's failure to cure a breach as set forth in this subsection is grounds for the immediate termination of this Addendum, the Core Services Agreement, and any other related agreements. In the event of a termination pursuant to this section, the provisions of Section VI.D shall apply. [This provision is not mandatory. If it is removed, Section VI.C.1 needs to be modified accordingly.]

D.Effect of Termination

1.Return or Destruction of Protected Health Information

Except as provided in Section VI.D.2, upon termination of this Addendum, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protecte3d Health Information.

2.Return or Destruction Infeasible

Section VI.D.1 shall not apply if the parties mutually agree that return or destruction of Protected Health Information is infeasible. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. If return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Addendum to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

VII.Notices

Any notices or reports required under this Addendum shall be provided to the notice contact and the copy recipient both via the U.S. Main or express courier and via facsimile, as provided below.

Insert contact information here.

[This provision is not mandatory.]

VIII.Miscellaneous

A.Regulatory References

A reference in this Addendum to a section in the Privacy Rule means the section as in effect or as amended. [This provision is not mandatory.]

B.Interpretation

Any ambiguity in this Addendum shall be resolved in a favor of a meaning that permits Covered Entity to comply with the Privacy Rule. [This provision is not mandatory.]

C.Amendment

The Parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191. [This provision is not mandatory.]

D.Conflict with Core Services Agreement

In the event that there is any conflict or inconsistency between the Core Services Agreement and this Addendum, this Addendum controls and amends the Core Services Agreement.

E.Survival

The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination of this Addendum.

F.Disputes

The Parties agree to make a good faith effort to resolve any controversy, claim or dispute between the Parties with respect to this Addendum. [This provision is not mandatory.]

G.No third party beneficiaries

This Addendum is not intended to confer any rights on any person other than the Parties. [This provision is not mandatory.]

Signatures of the parties follow

ACKNOWLEDGMENTS & CONTRIBUTORS

The Board of Directors of the Pennsylvania eHealth Initiative gratefully acknowledges the significant contributions of many individuals and organizations that have assisted in the development of this White Paper. In particular, the Board thanks William "Buddy" Gillespie, Steve Fox, Esq. (Chair of Post & Schell's Information Technology Group and Co-Chair of the firm's Data Protection Group), Mark Jacobs, and Anthony Wilson for serving as Chairs of the effort, as well as Martin Ciccocioppo and Mark Stevens for their guidance and leadership throughout the project. Members of the PAeHI Local Health Information Exchange Special Interest Group, the PAeHI Policy Committee and the PAeHI Business Analysis and Technology Committee all deserve thanks and congratulations for each Groups' efforts through numerous conference calls, e-mail revisions and two All-Committee event breakout sessions to collaboratively research, outline, draft and revise this White Paper.

The Board would also like to convey a special thanks to Glen Marshall, executive editor of the White Paper and Principal, Grok-A-Lot, LLC, for his exceptional effort, command of the topic and for the quality of his work. The Board would also like to thank Lisa Gallagher, Senior Director for Privacy & Security for HIMSS for her expertise and guidance; Robert Mitchell, Managing Editor of ADVANCE Magazine for his significant and timely editorial contributions and Highmark's marketing department for its proofreading support.

Finally, the Board acknowledges the below specific individuals, whose significant contributions merit individual recognition:

Denise Abraham, Washington PHO, Inc.
Matt Aisef, Wellogic
Don Bechtel, Siemens
Mike Berry, HLN Consulting, LLC
Gary Christoph, Northrop Grumman
Elizabeth Evans, Coker Group
Sarah Foust
Dawna Gardner, Blue Cross of Northeastern Pennsylvania
Alexandra Goss, Governor's Office of Health Care Reform
Linda Hogan, Commonwealth Medical College
John P. Houston, University of Pittsburgh Medical Center
Kathryn J. Magar, WellSpan Health
Elliot Menschik, HxTechnologies, Inc.
Sean O'Rourke
Max Reverman
Sue Salkowitz, Principal Salkowitz Associates, LLC

Copyright PAeHI, 2009

Contributors (continued)

Kim Slocum, KDS Consulting, LLC
Jay Srini, UPMC Health Plan
Mark Stone, 3M Healthcare
Andrea B. Thomas-Lloyd, Lancaster General
Jim Walker, Geisinger Health System
Mark Wallin, DocSite
Suzanne Weaver, Neshaminy Manor
Stephen Young, Neshaminy Manor
Jim Younkin, KeyHIE/Geisinger Health System
Yeva Zeltov, Pennsylvania Health Information Management Association
Cherie Zercher, Medicity, Inc.

THE PENNSYLVANIA EHEALTH INITIATIVE

BOARD OF DIRECTORS

2009

Martin J. Ciccocioppo (Chairman), The Hospital & Healthsystem Association of PA
Jay Srini (Vice Chairman), UPMC Health Plan
Darlene M. Kauffman (Secretary), Pennsylvania Medical Society
Scott Gillam (Treasurer), Highmark, Inc.
Kenneth D. Coburn, M.D., Health Quality Partners
Sharon L. Dorogy, The Children's Institute
Sen. Mike Folmer, Pennsylvania Senate
Dan Jones, Quality Insights of Pennsylvania
Don Levick, M.D., Lehigh Valley Hospital
Ellen Marshall, Camden Area Health Education Center (AHEC)
Philip W. Magistro, Governor's Office of Health Care Reform
Elliott Menschik, M.D. Ph.D., HxTechnologies Inc.
Jean B. Stretton, M.D., Gateway Medical Associates

Ex Officio Members:

Steve Fox, Post & Schell, PC
William "Buddy" Gillespie, WellSpan Health System
Mark J. Jacobs, WellSpan Health System
James M. Walker, M.D., Geisinger Health System
Robert Torres, Pennsylvania Department of Health
Donald F. Wilson, M.D., Quality Insights of Pennsylvania

PAeHI Staff:

Mark Stevens, Executive Director, Pennsylvania eHealth Initiative
(610) 363-2588, markwstevens@verizon.net

ABOUT THE EDITORS

Executive Editor

Glen F. Marshall
Principal
Grok-A-Lot, LLC
Information Technology Consulting
https://www.grok-a-lot.com

Glen F. Marshall is an information technologist with over 42 years' experience in healthcare systems architecture, development, implementation, operations and support. His specialties include healthcare information security, privacy, infrastructure, and standardization. He is a member and leader for numerous international healthcare standardization organizations. Now the Principal Consultant for Grok–A–Lot, LLC, Glen previously worked for Siemens Health Services and Shared Medical Systems as the Standards & Regulations Manager and IT Architect.

Contributing Editor

Bob Mitchell
Managing Editor
ADVANCE for Health Information Executives
rmitchell@advanceweb.com
www.advanceweb.com

Bob Mitchell is a member of the Pennsylvania e-Health Initiative. He is the managing editor at ADVANCE for Health Information Executives, a monthly, national health IT publication, where he is responsible for day-to-day management of the magazine's editorial staff and article assignments to CIOs and other senior-level IT executives in health care. He also maintains relationships with professional IT trade associations who provide the magazine with source material and author sources.

Mr. Mitchell has more than 18 years of editorial and management experience. He holds a Bachelor of Science degree in Journalism from Southern Connecticut State University in New Haven, Conn. He also studied theology at The Lutheran Theological Seminary in Philadelphia.

Copyright PAeHI, 2009

Pennsylvania eHealth Initiative
PO Box 8820
Harrisburg, PA 17105-8820
www.paehi.org

Copyright PAeHI, 2009