Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

2014
Contents

Introduction .................................................................................................................. 3
Executive Summary ...................................................................................................... 4
Key Definitions ............................................................................................................. 5
  Concepts, Stakeholders ......................................................................................... 5
  Personal Health Information .................................................................................. 6
  Key Staff .................................................................................................................. 7
Landscape and Roadmap – Current and Future ......................................................... 9
  United States National Landscape ...................................................................... 9
  Pennsylvania ........................................................................................................... 14
  Benchmarks from National Efforts and Other States ........................................... 15
What Is Currently Required? .................................................................................. 17
  Policies: Legal, Regulatory, Organizational, and Personal ................................ 17
  Conforming to Policies and Controlling Risk ......................................................... 24
  Workforce Considerations ..................................................................................... 27
Enabling the Solutions .............................................................................................. 29
  Best Practices ......................................................................................................... 29
  Stakeholder Education .......................................................................................... 30
  Key Technical Properties ....................................................................................... 31
  Demonstration and Model Projects ...................................................................... 32
  Emerging Areas of Risk and New Compliance Challenges .................................. 32
    Cloud Hosting
    Cyber Security Insurance and Cyber Attacks
    Mobile Device Management (BYOD)
    Physician and Patient Portals
    Checkbox Compliance
    Convergence of HIOs and Social Media
    Disposal of PHI
    PHI Ownership and Proprietary EHRs/HIEs
    Business Intelligence and Data Analytics
    Backup and Disaster Recovery for HIOs

Addressing Barriers to Solutions ........................................................................... 46
References .................................................................................................................. 48
Appendices ................................................................................................................ 50
  Federal 2011 DURSA ............................................................................................ 51
  AMA Sample BAA ................................................................................................ 99
  Pennsylvania Opt-Out Form .................................................................................. 117
  Ensuring Privacy and Security of Health Information Exchange in PA,
    Slides from May 14, 2014 PAeHI Summit ......................................................... 118
Acknowledgements & Contributors ....................................................................... 132
Introduction

The Pennsylvania eHealth Initiative (PAeHI) is a not-for-profit founded in 2005 by the state’s leading health care organizations to transform health care by fostering the broader adoption of electronic health records and health information exchange.

In the sharing of patient data, PAeHI recognizes that robust patient privacy and security protections are essential to build and maintain the necessary level of trust among patients, health care 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 health care data privacy and security for electronic information exchange. The key purpose is to help health care providers achieve acceptable data privacy and security assurance for health care consumers, while minimizing cost and confusion. It does not discuss the much broader issues of non-electronic health care data privacy or general security technology.

The regulatory and marketplace landscape has been evolving in a dramatic fashion since the first edition of this white paper in 2009. In order to set that stage, the legal and regulatory sections have been made more in depth to serve as a tool for the provider community. Pennsylvania has also established an independent Commonwealth agency that has been tasked with governing the state health information exchange network of services, establishing and maintaining a common consent registry for patients to opt-out of the exchange, and promoting interoperability within the state HIE marketplace. Much of the updated material in this white paper is reflective of that effort, and is offered here as guidance to the health care community at large.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Executive Summary

Patients are unlikely to share sensitive health information unless they are confident that their provider will honor their confidentiality. Similarly, health care entities are unlikely to join a health information exchange if they are not confident that their medical records will be kept safe and that the data will be flowing securely.

A key factor in achieving a high level of trust and compliance among individuals, health care providers, and other health care organizations participating in a health information exchange is the development of, and adherence to, a consistent and coordinated approach to privacy and security. Clear, understandable and uniform principles are a first step in developing this approach to privacy and security while building trust, which are all essential to the realization of the considerable benefits of HIE.

It can be a challenge to adopt clear and uniform privacy and security principles in a legal landscape that seems inconsistent and restrictive. Absorbing those principles into a sustainable business model that hits all its required regulatory marks requires strong leadership and the will to get it done to both support the business goals and serve the patients and consumers of Pennsylvania.

In 2012, the Commonwealth established the Pennsylvania eHealth Partnership Authority as the governance entity for HIE in the state. The Authority is moving forward with all the mandates contained in its founding legislation to provide uniform standards and agreements that are produced in concert with stakeholders, along with freely distributed consumer outreach tools and a state consent registry.

PAeHI sees this as the first vital step in Pennsylvania achieving a truly interoperable health information exchange network that both supports and expands the market for such services. The broad topic discussions and outlines contained in this white paper are presented as a tool to spur further thinking about the appropriate methods to interface with the legal requirements as to electronic health information privacy and security, the specific requirements within Pennsylvania, and the workplace challenges of technical and administrative implementation.
**Key Definitions**

**Concepts**

**Privacy**
(1) The right to have all records and information pertaining to health care treated as confidential.
(2) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue, unauthorized, or illegal gathering and use of data about that individual.
(HIMSS, 2006)

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

**HITECH Act**

Title XIII (Health Information Technology), Division A, pp 112-165 and Division B, pp 353-398 of ARRA may be cited as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act."

**Omnibus Final Rules**
The Omnibus final rule clarifications were released in January 2013 to provide additional rulemaking around the HIPAA Privacy and Security Rules. The Omnibus rule was based on statutory changes under the HITECH Act and the Genetic Information Nondiscrimination Act of 2008 (GINA).

**Meaningful Use**
A concept included in the HITECH Act that allows for incentive payments to providers for the deployment and appropriate use of electronic health records.

**Pennsylvania eHealth Information Technology Act**

This Act, also known as Act 121 of 2012, established the Pennsylvania eHealth Partnership Authority (Authority) as an independent agency of the Commonwealth and the governance body for the statewide technological health information exchange network it was to build.

**Stakeholders**

**Consumer**
A person who obtains health care services or, by extension, a person who represents a patient such as a parent or legal guardian.
Covered Entity (CE)
HIPAA defines covered entities as health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. These transactions are usually billing and payment for services or insurance coverage. An entity may be a “hybrid entity” that performs both covered and noncovered functions. The HIPAA Privacy Rule only applies to Covered Entities.

Patient
The direct recipient of health care and the subject of associated health care 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 exchange. This may be a mechanism or organization designed to share health care information electronically across organizations within a region or community, or it may be the technological act of sharing such electronic information.

HIO
Health information organization. A health information technology infrastructure or the organization establishing such a system to ensure the secure digital exchange of health information among participants engaged in the care of patients.

Provider
Any person or entity that supplies health care services for patients.

Stakeholder
A general term which includes consumers, patients, health plans, HIEs, HIOs, providers, 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. EHRs may be connected in an interoperable fashion with other records systems. EHRs are expected under “Meaningful Use” requirements.

EMR
A digital version of traditional paper medical charts. These records do not normally have the ability to send data outside the medical practice, or become interoperable with other record systems.

Encryption
Encryption is the conversion of data into a form that cannot easily be understood by unauthorized people. Authorized people or machines use a decryption algorithm to read the data.
The more complex the encryption algorithm used, the more strongly encrypted the data is considered to be. Only NIST encryption methods are accepted as adequate protection of PHI.

**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.

**Personal Health Record (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.

**Personally Identifiable Information (PII)**
Information that can be used to distinguish an individual’s identity, usually considered demographic information. Some PII, such as social security numbers or Medicaid IDs, is considered sensitive PII.

**Protected Health Information (PHI)**
Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), any personally identifiable health information about a person, regardless of format. The HIPAA Privacy and Security Rules specify the protections.

**Key Staff**

**Business Associate**
A person who, on behalf of a covered entity or an organization in which the covered entity participates, creates, receives, maintains, or transmits protected health information. Business Associates have now been required to be fully HIPAA compliant in the course of their employment, and have become legally liable for the mishandling of PHI.

**Compliance Officer**
An employee whose responsibilities include ensuring that the company complies with its outside regulatory requirements and internal policies. This position can oversee the Board of Directors, management, and employees. While these job functions have traditionally been under the corporate in-house counsel, there has been a movement in recent years to have compliance be its own position.

**Privacy Officer**
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:
- Access
- Amendment
- Disclosure accountings
Supplemental protections
Confidential communications
Authorizations for additional uses

Security Officer
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.
Landscape and Roadmap – Current and Future

The health care industry has had many spirited discussions regarding privacy and security from both the provider and patient perspectives since HIPAA was enacted in 1996. The issues surrounding privacy and security continue to challenge all stakeholders regardless of technological sophistication, particularly those involved in the direct delivery of care. This tension between privacy and security requires collaborative solutions that fairly balance the competing interests between security implemented from a business perspective and with an eye to the bottom line, and the privacy rights and expectations of individuals as to their medical information.

United States National Landscape

The HIPAA Privacy Rule was effective April 14, 2003 for the majority of health organizations. The Privacy Rule establishes national standards for the safeguarding of medical record privacy, sets conditions on uses and disclosures, and codifies the basic rights that individuals have over their health information. Covered entities may disclose this information for treatment, payment, or health care operations without specific patient authorization. Only these “covered entities” are subject to the Privacy Rule.

The HIPAA Security Rule became effective April 21, 2003 with some later compliance dates for specific entities. While the Privacy Rule covered all records, written or electronic, the Security Rule specifically deals with electronic health information. The Security Rule requires physical, technical, and administrative safeguards that work in concert to ensure the integrity and security of the protected health information (PHI).

The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted as part of the 2009 American Recovery and Reinvestment Act (ARRA). HITECH included incentive payment systems aimed at increasing the adoption of electronic health records, known collectively as “Meaningful Use”. Health information exchange and associated technologies emerged as important for health care entities to comply with HITECH and receive the stimulus funds. The intent was to improve efficiencies in the U.S. health care arena through improved care coordination, reduction of health care disparities, and improvement of both public and population health, and thus reduced overall costs. HITECH made grants available to the individual states to establish statewide HIE networks, founded the Office of the National Coordinator (ONC) to oversee the growth of health information technology (HIT) on a national level, and established several Committees that would be involved in establishing and recommending policy frameworks. The HITECH Act also required covered entities to report data breaches affecting more than 500 people to both HHS and the media, in addition to the required notifications to the affected individuals. HITECH extended all HIPAA Privacy and Security Rule provisions and their associated civil and criminal penalties to all of the covered entity’s business associates.

These provisions of HITECH were an attempt to accelerate the adoption and use of electronic medical records, while also taking steps to tighten the regulations requiring adequate security of those records. This interwoven system of incentives and pressure, a carrot and stick approach,
has met with mixed success in promoting the mandated conversion to electronic health records. HITECH was meant to put some regulatory teeth into the HIPAA privacy and security provisions, with enforcement and penalties applying directly to business associates. A 2009 HIMSS survey showed that security costs accounted for 1% or less of health care entity’s budgets, with no change in spending since 2008. Health care as an industry has lagged behind other industries in their thinking about and implementation of upgraded privacy and security standards. While conversion to EHRs has promoted a tremendous growth in the amount of electronic health data available, with a parallel increase in the possibility of accidental or malicious exposure of that data, the appropriate protection of that information has been developing slowly due to both technological challenges and budgetary pressures. The data breach notification requirements that HITECH mandated also put pressure on both health care providers and technology providers to avoid the costs and negative publicity attendant on such notifications.

In January 2013, the Omnibus Final Rule clarifications were released to provide additional rulemaking around the HIPAA Privacy and Security Rules. The Omnibus rules were based on statutory changes under the HITECH Act and the Genetic Information Nondiscrimination Act of 2008 (GINA). They enhanced patient’s privacy protections, provided individuals new rights in their health information, and strengthened the government’s ability to enforce these rights and protections. The Omnibus strengthened the privacy and security portions of HIPAA by enhancing patient rights on records access and restricting certain disclosures to health plans; it modified the required notices of privacy practices, strengthened restrictions on fundraising and marketing practices, required specific authorization for sale of PHI and research uses, and expanded the direct enforcement of HIPAA requirements and penalties directly to all business associates. It adopted changes to the enforcement rules that increased monetary penalties and applied a new tiered civil monetary penalty standard for breaches. The Omnibus modified HIPAA to conform with GINA to include a person’s genetic information under the umbrella of protected health information, and modified the breach notification for unsecured protected health information by replacing the rule’s “harm” threshold for notification with a more objective standard that presumes a breach until proven otherwise according to a list of factors. These changes led many HIOs to do an in depth evaluation of all of their legal agreements with their contractors and vendors, and to set about rewriting their existing Business Associate Agreements (BAA) to bridge the gap between the old standards and the new. The compliance date for the Omnibus changes was September 23, 2013, with transition time available for old BAAs.

In October 2013, the insurance marketplaces required by the Patient Protection and Affordable Care Act (ACA), which had been signed into law in March 2010, became active. These online marketplaces were plagued with technological glitches, something that was not unexpected considering the sheer magnitude of the federal effort and the number of states that had ultimately opted out of establishing their own websites and state programs. The ultimate societal and marketplace outcome of this program is still to be determined, but it has kept health information technology in the news and under the microscope. Unfortunately, it has also meant that a lot of the national conversation has turned to insurance marketplaces and deadlines and away from state and regional health information exchange efforts.
As of early 2014, the largest piece of federal regulation still outstanding is the expected rulemaking covering Accounting of Disclosures, a piece deliberately omitted from the Omnibus. HITECH required under the HIPAA Privacy Rule that patients be given the ability to request an accounting of disclosures about their medical records, to get a list of all the places that their medical records were sent to and viewed by outside of their provider. In 2011, HHS issued a notice of a proposed rulemaking to implement the requirement under HITECH that the accounting of disclosures right also apply to disclosures of electronic health records. HHS proposed expanding the rule to also require that an “access report” be made available to a requesting patient covering what people inside of their health care entity saw and accessed from their electronic records, and for what purpose. Despite comment periods, Senate hearings, and much discussion, this final rule has not yet been issued due to the difficulties in balancing the administrative and monetary burden of implementing these rights with the interest of the affected individuals.

Regulations

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

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

Ongoing Standards Work

Technical standards in HIE concerning privacy and security focus on encryption, identity proofing and authentication, audit records, and secure transmission. EHR vendors seeking certification for their systems to be used by providers and hospitals participating in the Meaningful Use program must meet these standards that were set by the ONC.

¹ The Departments of Education and Health and Human Services 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)
The ONC established the Health IT Standards Committee (HITSC), which uses workgroups and sub-committees to concentrate on particular subjects. HITSC receives recommendations from the Privacy & Security Standards Workgroup. Stakeholders of the HIE community comment on Meaningful Use standards before official adoption. The comments and responses may be reviewed in the published final rule. If time allows, reading this material is an excellent tutorial on the current tensions in the field that the final rule attempted to balance.

The ONC requires the standards listed below for Meaningful Use Stage 2 (MU2).

**Encryption**

A handler of health care information should never let it sit at rest without encryption, especially if it is on a mobile device or a storage unit. The encryption standard required in MU2 is tied to secure messaging for communicating with patients (DIRECT). This in-transit requirement doesn’t dilute the need for encryption of information not being transmitted, i.e. at rest. Laptops and other hardware are expected to have data encryption capability. This is particularly important in the event of any needed mitigation in the event of a data breach.


- **Symmetric Keys** – Advanced Encryption Standard (AES), Triple-DES Encryption Algorithm (TDEA), Escrowed Encryption Standard (EES)
- **Asymmetric Key** – Digital Signature Standard (DSS), Secure Hash Standard (SHS)

**Identity Proofing and Authentication**

Before issuing credentials to a user who will be accessing health care information, the issuer should be as sure of the user’s identity as possible. Each time that user accesses the system containing health care information they should have to prove their identity through authentication.

The National Institute of Standards and Technology (NIST) developed and documented many of the standards endorsed by ONC. For the purposes of identity proofing and authentication the health care industry refers to NIST 800-63 as a guide. The document describes several Levels of Assurance (LoA). ONC recommends NIST level 3 adoption and use.

**Audit Records**

Rather than specifying a technology standard for audit records, the ONC refers vendors to a document from the American Society for Testing and Materials (ASTM). Certain sections and parts of sections from ASTM E2147-01 (2009) discuss auditable events. Records of these events will help privacy officers reconstruct access and track changes to health care information. HIPAA audits began under the leadership of the Office of Civil Rights and are ongoing.
Transmission

MU2 requires providers to share information with patients. The DIRECT Project, sponsored by the ONC, developed a secure method of transmitting health care information over the internet through secure email. The Applicability Statement for Secure Health Transport version 1.1 contains the current specifications for DIRECT. Using Domain Name System (DNS) and Lightweight Directory System Protocol (LDAP) technology is specifically called out by ONC. Certified EHRs must have the capability to provide DIRECT to their users.

Meaningful Use 2 versus Meaningful Use 1

HITECH left some aspects of security implementation unclear. The final MU2 rules provided more clarity on what organizations should do to encrypt data on end-user devices, and what data should be collected for appropriate audit purposes. This was all done within existing industry and governmental standards, and should have taken the perceived ambiguity out of planning implementations to be compliant. Thorough and honest risk assessments are still the keystone to all security implementation planning efforts. Meaningful Use compliance audits have begun and are ongoing.

Due to the administrative effort, technical effort, and costs involved in becoming MU2 compliant, some organizations may choose to stop at MU1. Some vendors have also found that they could not achieve above MU1 certification. Stage 1 focused on the transition to electronic health records, while stage 2 focuses on actual information exchange and patient engagement. Some providers may find themselves forced to upgrade to an MU2 compliant system when the vendor for their MU1 system has ceased operations or stopped supporting the software. Entering the world of HIE with a system stuck at MU1 could be a liability risk, as information could be transmitted as unsecured data.

Marketplace

The vision for HIE in Pennsylvania is to ultimately strengthen the health care system and improve both health care delivery and health care outcomes. This would be achieved through the timely, secure and authorized exchange of patient health information among all health care providers willing to participate, including those providers who serve the vulnerable, underinsured, or uninsured populations, plus Medicare and Medicaid patients living in both rural and urban settings. To achieve this vision, adoption rates of health information exchange must increase across the state.

An alternate method of transmitting PHI is through the use of secure email systems, termed DIRECT. DIRECT was an initiative started and promoted by ONC to enable an alternate low-cost PHI transmission standard for health care providers. DIRECT email accounts are usually provisioned and maintained by health information service providers (HISPs). The ability to support DIRECT clinical messaging is required for MU2 certified EHRs.
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 infrastructure. In July 2011, Governor Tom Corbett established the Pennsylvania eHealth Collaborative (Collaborative) by executive order. The establishment of the Collaborative was the culmination of several years of effort within Pennsylvania by many and various stakeholders, from both within PAeHI and from within the internal agencies of the Commonwealth. Pennsylvania received a $17.1 million dollar grant under the HITECH provisions to establish and promote HIE within the Commonwealth, and the Collaborative became the steward of that grant. In July 2012, Act 121 of 2012, known as the Pennsylvania eHealth Information Technology Act, was passed unanimously by the General Assembly. The Act established the governing body for HIE in Pennsylvania, the Pennsylvania eHealth Partnership Authority (Authority), and outlined the appointment of a Board of Directors to serve as the agency oversight body. The Collaborative transitioned to the Authority, and began the process of building a statewide HIT infrastructure known initially as the Community Shared Services (CSS).

Act 121 established Pennsylvania as an opt-out state, and directed the Authority to promulgate a standardized opt-out form that would serve the entire state. The Authority was also specifically directed to establish governing policies and procedures, develop and maintain interoperability standards, construct and maintain a master provider index, build and maintain an opt-out consent registry, and produce consumer educational materials about HIE. The Authority has taken a collaborative approach to the production of needed polices, agreements, consumer materials, and forms. This marketplace-focused approach established by the Act has not produced complete consensus, but it has yielded a framework ultimately designed and requested by the majority of stakeholders.

Pennsylvania has the unenviable position of being a state that is termed HIPAA-plus. HIPAA-plus states have state laws that are more stringent about certain areas of health care information privacy and handling than the floor that HIPAA establishes. These areas are referred to collectively as super protected data (SPD). There are additional safeguards afforded to the “super protected data” categories under current Pennsylvania law that include, among others, mental health records, HIV/AIDS records, and substance abuse records. This distinction produces quite a strain on the Pennsylvania HIE marketplace, as such SPD is often irrevocably embedded amongst other health information, where it is either overlooked and the record is allowed to be shared – producing an unintentional violation of state law through incidental release of SPD – or the health care entity takes the most risk-averse stance and does not circulate any records that cannot be guaranteed as not containing any SPD. Current software technology does not allow the level of granularity of data segmentation or masking that is required to completely and consistently meet the consent requirements of a HIPAA-plus state. While there are federal efforts to advance such segmentation standards (Data Segmentation for Privacy, S & I Framework), they are as of yet unavailable for marketplace absorption. As this sort of segmentation is also required to comply with SAMHSA Part 2 requirements as to substance abuse treatment programs, health care entities are eagerly awaiting such capabilities.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

The Authority plans to partner with stakeholders to consider the possibility of amending Pennsylvania law to be HIPAA compliant rather than more stringent than HIPAA. This would release some of the pressure that the Commonwealth HIE marketplace labors under, and would also make interstate electronic health information exchange easier.

Pennsylvania has a dedicated personal information breach notification act (73 P.S. §§ 2301, et seq.) that went into effect in June 2006. The notification requirements of the Act are triggered when there is a breach of the security of a computerized data system “to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.” This Act has been read to cover medical records where a person’s name can be connected to a social security number or a Medicaid/Medicare ID number, driver’s license number, or other state or federally issued number that identifies that individual. It requires notification of the breach without unreasonable delay by the business entity that was holding the information. Pennsylvania HIOs must take this statute into account when writing their breach notification protocols, as well as the HIPAA notification standards.

**Benchmarks from National Efforts and Other States**

The National Governors Association Center for Best Practices created the State Alliance for e-Health in 2007. This collaborative body was created to improve the nation’s health care system through the efficiencies that the adoption of HIT can create. The NGA Center was awarded a contract from the Office of the National Coordinator for Health Information Technology (ONC) to establish this alliance. This group was active in the eHealth realm in 2010 and 2011, until their ONC contract ended, and has a variety of materials from that timeframe available on their website. Since 2011 the NGA has focused their health care efforts mostly on the implementation challenges of the state insurance exchanges required by the ACA.

The Standards and Interoperability Framework (S&I) is a forum created by the ONC where health care stakeholders can hash out interoperability challenges, and have the opportunity to establish standards, specifications, and other implementation guidance to help facilitate effective health information sharing in the real world. There are various S&I initiatives going on continuously that members can involve themselves in. There is also a wealth of information available to organizations that join as members.

The Markle Foundation works to realize the potential of information technology in improving the lot of all Americans. Their work in the health care arena has focused on advancing HIT through the development of the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange. This Framework was developed through a consensus-driven process and collaboration with more than 100 public and private organizations. The documentation around this framework is freely available through their website, and covers such topics as authentication of system users, medication history standards, model privacy policies and procedures, record locator services, and an HIE architecture implementation guide.

As the media reports more and more cases of consumer data breach around the country, various states have stepped up efforts to put into law at least basic notification regulations requiring that
ensuring Privacy and Security of Health Information Exchange in Pennsylvania

consumers be told when their personal information has been breached. These laws normally also cover medical information. California became the first state to pass an online breach notification law. In 2002, California passed a law requiring consumer notification of the security breach of any personal information regardless of what industry or agency held it. They have followed this up in 2013 by also protecting passwords for online accounts and the disclosure of online tracking of a consumer’s browsing activity. Such regulatory activity points up the lack of a national security breach standard; requiring business to therefore contend with a patchwork of different state privacy laws. A “Consumer Bill of Rights” has been proposed at the federal level, but has not become law.

The American public has become very used to having unfettered mobile access to their data via smart phones, tablets, and cloud services. All of these new data pathways have their own security issues, and data does not stop – or even pause – at state borders where the privacy laws and security standards may change. This is another reason why marketplace participants would be best served by strict attention to their internal privacy and security standards, and where cost-cutting measures may serve short-term budget goals but will not serve any industry in the long run. Every day the public is treated to more stories of their personal data being mishandled or stolen. The Neiman Marcus breach went on for 8 months and exposed about a million consumers. The Target debacle is still being totaled up at 8 million consumers and counting. These companies are paying and will pay a price for the holes in their security. While these examples are from the financial world, not the health care world, the health care industry must take note of the financial and business credibility fallout. Consumers can understand why criminal enterprises would try to get at their financial information. What patients will not understand or forgive is how their trusted health care providers could have allowed their sensitive personal health information to escape through inattention, lack of appropriate protocols, or unwillingness to operate strong security controls.
What Is Currently Required?

As described above, health care providers are subject to a number of state and federal laws related to the 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 viable Health Information Exchange.

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 HIO/HIE participants, providers’ policies, and patient-specific disclosure consents and restrictions.

Trust Agreements Among Care Providers

The parties associated with HIOs 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.

In Pennsylvania there has been an effort to establish a trust community through standardized agreements. These agreements include a participation agreement, a data usage and reciprocal sharing agreement (DURSA) between the Authority as the governance agency and the participants (HIE or HIO entities), a business associate agreement for the participants to use with their member organizations, a DURSA to be used between the participants and the member organizations, and three standard policy documents outlining privacy standards and security policies. These documents were written in collaboration with stakeholders in an iterative process. All agreements used federal templates as a starting place, and incorporated the eight S&I Framework Privacy and Security principles. These principles are:

- Individual Access – Individuals should be provided a simple and timely means to access and obtain their health information in a readable form and format.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Correction – Individuals should be provided with a timely means to dispute the accuracy or integrity of their health information, and to have erroneous information corrected or to have the dispute documented if their correction request is denied.
- Openness and Transparency – There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their health information.
- Individual Choice – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their health information.
- Collection, Use, and Disclosure Limitation – Health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose and never to inappropriately discriminate.
- Data Quality and Integrity – Persons and entities should take reasonable steps to ensure that health information is complete, accurate, and up-to-date to the extent necessary for the person’s or entity’s intended purposes and has not been altered or destroyed in an unauthorized manner.
- Safeguards – Health information should be protected with reasonable administrative, technical, and physical safeguards to ensure confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- Accountability – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

Adoption of privacy and security policies is essential to establishing the public trust necessary for effective electronic exchange of health information. Harmonizing the marketplace through establishment of a trust community with standardized forms and procedures will not reduce competition, nor will it cost any particular organization marketshare. The journey through the initial efforts, however, may be a rocky one, as organizations struggle with their own business decisions and internal corporate cultures that may not see such cooperation as business or profit friendly. The implementation of these principles needs to evolve in combination with technological advances that allow for greater security, and legal assistance for agreement composition and review. These principles are not legal requirements, and do not represent regulatory requirements. However, where the principles set higher expectations than current legal requirements, adherence to the principles is encouraged.

**Consumer Consent for Disclosures of Health Information**

Most consumers want health care 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. However, it is worth noting that these consumers wish to know that only their chosen network of providers is accessing their information. That is, the majority of consumers want to control their health care information by delegating that control only to people and organizations they know and trust. The world has become digitized, and any consumer with a television knows that information is currency on the open market. We no longer live in a world where people do not expect to have some control over their personal information.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

or are normally willing to simply delegate all control and believe that their information will be handled and safeguarded appropriately.

Under the HIPAA Privacy Rule, information may be disclosed for treatment, payment, or health care operations without prior consent from the consumer. All other uses require patient consent. In addition:

- Health care providers must (except in an emergency) obtain the consumer’s written acknowledgment of receipt of the notice of privacy practices (NPP). This NPP must conform to current guidelines as outlined by the Omnibus final rules.

- A consumer may request that information about medical procedures and contacts that were completely self-paid be withheld from sharing with insurance companies.

- A health care provider must provide within a reasonable timeframe an “Accounting of Disclosures” to a patient upon request.

In conformance with HIPAA, 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 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., co-morbidities, may be disclosed in accordance with the HIPAA Privacy Rule. Under SAMHSA regulations, even minors must sign a consent document before information is disclosed to their parents. The mandated consent must include the following elements:
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- 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 a consent for disclosure is required. But under SAMHSA Drug and Alcohol provisions, oral revocation can be sufficient.

In Pennsylvania, health information exchange initiatives are faced with the challenge of balancing the needs of privacy advocates with those of health care providers as they develop policies and procedures related to patient consent and control, taking into account both federal and state oversight. Pennsylvania was established as an opt-out state by the Pennsylvania eHealth Information Technology Act (Act 121 of 2012), and the Authority was directed to promulgate a standardized opt-out form. This form will serve as the consumer-facing form for Commonwealth citizens to opt-out of the statewide electronic exchange network. This form does not cover the specially-protected categories of health information created by various Pennsylvania statutes, mental health information, HIV/AIDS treatment, and drug and alcohol abuse treatment. Patients must give specific doctor-to-doctor consent for those categories of medical records to be shared, and must also provide specific revocation of those consents if no expiration was stated.

**Business Associate Agreements (BAAs)**

The HIPAA Privacy Rule requires that health care providers have business associate agreements with their providers. The Omnibus final rules extended compliance obligations and liability directly to business associates regardless of the wording of any contractual documents in place. If a subcontractor receives or accesses PHI as a part of their delegated function, then that person is a business associate, and will be held to HIPAA compliance standards. Thus, status as a business associate now flows down the chain through whatever contracts are in place to land upon whatever person is actually handling that PHI. BAs must comply with all applicable parts of the HIPAA Security Rule, not use or disclose the PHI in any way that would violate the HIPAA Privacy Rule, be aware of and follow breach notification policies, and use and disclose...
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

PHI only as permitted to by their BAA. Businesses employing such BAs need to be aware that compliance liability will also flow back up the chain of command from a BA who has caused a breach of information, back to the supervisors, Security Officers, compliance personnel etc. who were contractually tasked with monitoring BA privacy and security training and compliance.

PAeHI urges providers to consult an attorney before preparing or signing a business associate agreement, and to choose an attorney with experience in this rather specialized area.

Data Use and Reciprocal Support Agreements (DURSAs)

A DURSA is an agreement that governs the exchange of health information between participants in a health information exchange. This comprehensive agreement was originally developed for use in the NwHIN federal exchange, and is intended to be a legally enforceable multi-party agreement that represents a framework for information exchange among a set of trusted entities. This agreement covers privacy and security obligations, permitted purposes for the data, duties of both submitting and receiving participants, participant breach notification, mandatory non-binding dispute resolution, and allocation of some risk. The purpose of the document is to obviate the need for any point-to-point agreements. This federal DURSA was produced in two versions (2009 and 2011), and is freely available as a template for organizations to absorb and tailor for their own use. The federal effort which replaced NwHIN, HealtheWay, is using the 2011 version as their own DURSA, the execution of which is required to participate in their federal gateway efforts. This agreement, while long and a bit intimidating to non-lawyers, is also written so as to absorb technology changes as they occur.

Pennsylvania has been promoting the usage of standardized DURSAs within its state-sponsored network. The iterative work on building this and allied documents is ongoing.

Risk Management

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 health care IT exists in an 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 health care 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 that should prevent unwise investment in security or privacy technologies based on popular demand, sales presentations, or sensationalist press reports. It is about much more than keeping hackers from stealing personal health information. Rather, it is critical to address such issues as:
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Protecting confidentiality of personal information
- Legal and regulatory compliance
- Safe provisioning of health care services
- Patient safety
- Avoiding medical errors
- Risk associated with portable technologies and cloud services
- The cost and benefit of protective measures

While the majority of risks can have negative impacts, risk analysis can also expose opportunities to enhance the quality of care, for example, by reducing wait times, providing consumers with additional access to their health data, and reducing medication conflicts through automated checks against a pharmacy 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 controls as components of good corporate governance
- Assist in meeting health care requirements and objectives
- Facilitate partnerships with other health care organizations to address the issues inherent in interoperability

Risk Management Framework

A risk management framework combines all the processes involved in realizing existing, as well as emerging opportunities in a manner consistent with public interest, human safety and the law, while managing adverse effects caused by the complexity of health care systems. It involves identifying, assessing and judging risks, assigning ownership of the risks, 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.

Such a framework’s complexity needs to match the scale and scope of a health care organization. Large-scale organizations may employ professional risk analysts or consulting firms; smaller organizations may use cookbook-like tools or toolkits made available from various standards organizations. 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 will identify risks, the financial consequences of a realized risk, and the likelihood of those risks occurring. They should be 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 health care organization.
In contrast, an ad-hoc approach to addressing newly identified risks may overlook the importance of existing risks. It creates its own 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 requirements under the guidance of a security operational framework standard. Documented techniques and methodologies exist for conducting organizational risk assessments, which draw from relevant best practices and industry guidelines or requirements such as those published by the National Institute of Standards and Technology (NIST, SP 800-30 rev1, 2012).

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

Health care has some particular threats not found in other IT systems:

- Medical data may be used to profile patients and negatively impact non-medical aspects of a patient’s life such as employability, credit, and life insurance availability.
- 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 goods.
- Poor patient and record matching involves the 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. This inadvertent exposure of the wrong medical records can be a HIPAA violation, depending on how the incorrectly retrieved records are then handled.
- Consumer’s privacy-protective behaviors can be a significant threat to patients’ well-being, as they may withhold relevant clinical data if they believe their privacy is not being respected.

Mitigation Strategies Overview

There are no “silver bullets” to address risks. Under the HIPAA Security Rule, appropriate standards and safeguards are categorized for easy consultation. HHS has also recently released a
security risk assessment tool to help providers in small to medium sized offices conduct appropriate risk assessments of their organizations.

- Administrative controls – Non-technical things that need to be done in the course of IT acquisition, implementation, and operation to provide assurances that privacy and security policies are being followed and enforced. These security measures protect the information and manage the conduct of the workforce in relation to the protection of that information.

- Procedural controls – Non-technical things that need to be done in conjunction with environmental, physical, and technical controls. This could include specifying the appropriate use of work stations, and allowing access to facilities based on roles.

- 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 barriers, such as locked doors or guard stations.

- Technical controls – Portions of an automated system purposed with enforcing compliance with privacy and security policies and meeting security objectives. This includes automated data transmission security and automated role-based access and auditing.

- Residual risk controls – Various non-technical measures taken 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/HIO, 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, communications need to be clearly explanatory about how the technologies work together to make their health care more efficient and safe, how their medical privacy will be protected, and what rights they have in that medical information. It does not behoove companies to underestimate the public outrage that data breaches cause, especially when the problem can be publicly traced back to a lack of appropriate standards or systemic failure to adhere to those standards. It also should be pointed out that the practice using an EHR is responsible for taking the basic steps needed to protect the information contained in that electronic health record, not the vendor or a contracted-with HIO. Security starts with the boots-on-the –ground who are routinely accessing and using the records.

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. In addition to the federal breach notification rules, Pennsylvania also requires such notifications under its Breach of Personal Information Notification Act (Act 94 of 2005), as do most other states.

**Conforming to Policies and Controlling Risk**

The Introductory Resource Guide for Implementing the Health Insurance and Portability Act (HIPAA) Security Rule (NIST 800-66, Rev 1) has not yet been updated since the Omnibus rules
were published, but it still stands as an authoritative resource for those entities that need guidance as to information security best practices.

Administrative Controls

HIPAA requires that entities adopt and implement policies and procedures to prevent, detect, contain, and correct any security violations. This would require entities to:

- Identify all relevant information systems – identify all systems that house PHI, including their hardware and software used to collect, store, process, or transmit such PHI
- Conduct risk assessment – conduct accurate and thorough assessment of the potential risks and vulnerabilities to the PHI held by the organization
- Implement a risk management program – implement security measures sufficient to reduce risks and vulnerabilities to an appropriate level consistent with the Security Rule
- Acquire IT systems and services – additional hardware, software, or services may be needed to adequately protect information
- Create and deploy policies and procedures – implement decisions concerning all controls selected to mitigate identified risks, create policies to clearly assign all roles and responsibility, create procedures to be followed to accomplish particular security-related tasks
- Develop and implement a sanction policy – apply appropriate sanctions for noncompliance of workforce members
- Develop and deploy the information system activity review process – implement process to regularly review audit logs, access reports, etc.
- Develop appropriate standard operating procedures – determine types of audit trail data and monitoring procedures that will be needed to produce reports
- Implement information system activity review and audit process – activate necessary review processes

Procedural Controls

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

- Accountability for following and enforcement of privacy and security policies, associating specific identities to those who are accessing IT system resources or data (role-based access). 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 to fulfill “accounting of disclosures” and “access report” requests.
• 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 generally 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.

The process of defining the required procedural controls should be part of the administrative controls defined previously.

**Physical and Environmental Controls**

In most cases, technical security measures exist alongside physical and environmental controls. They may supply adequate protection, making more sophisticated security technology unnecessary. Risk analysis will help determine those choices.

Physical controls inhibit unauthorized access. These facility access controls may 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 organizational environment of an IT system that may mitigate threats. Examples of environmental controls include:

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

**Technical Controls**

The HIPAA Security Rule does not specify requirements for the types of technology that providers must implement as PHI safeguards. Instead of being forced to adhere to specificities, providers have to decide which security measures and technologies are reasonable and appropriate for implementation under their circumstances. The categories of possible technologies are:
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Access Controls – unique user identification, emergency access procedures, automatic logoff, encryption and decryption of PHI, password expiration
- Audit Controls – mechanisms to record and monitor activity in systems containing or using PHI
- Data Integrity – mechanisms to authenticate PHI as unaltered
- Person or entity authentication – implement procedures to authenticate any person or entity seeking access to held PHI
- Transmission Security – guarding against unauthorized access to PHI during transmission through integrity controls and encryption

Those who acquire or build health care information systems are responsible for ensuring all technical safeguard aspects are in place, and for enforcing security policies and procedures.

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 – usage of trust agreements and/or business associate agreements. The HIPAA Privacy Rule requires health care providers to have business associate agreements with vendors.
- Insurance – Transferring the financial consequences of risk to an insurance company, essentially pooling risks with other institutions.
- Risk acceptance – Some risks are so unlikely, even if they may have catastrophic consequences, that it may be prudent merely to accept them.

Workforce Considerations

At the end of the day, information security is really about people. The security systems and privacy controls are only as strong as the people using them. Staff members are usually well intentioned when they share health information as part of their jobs, but it still takes appropriate and repeated training to increase the probability that the staff will remember and follow proper procedures.

Many health care organizations seem to face an uphill battle in their efforts to prevent data breaches while still allowing the crucial medical information to flow between the providers who need it. The Ponemon Institute’s Study on Patient Privacy and Data Security (12/2012 and 3/2014), shows that employee mistakes and negligence continue to be a significant cause of data breaches. This 2012 study showed that employee training is the most common activity performed by the reporting organizations, but it was not effective in reducing the levels of reported insider
negligence. The loss of a computing device caused 47% of the breaches. Employee mistakes or negligence follows at 42% of reported data breaches. A trend affecting this appears to be the upward trend of mobile employer and employee-owned devices putting patient data at risk. A full 81% allowed employee-owned mobile devices (smartphones, tablets, laptops) to connect to their networks for at least email access. Half of all employees were bringing their own unsecured devices to their workplaces and using them. This is a new and increasing risk to the security of those enterprise systems.

The activity reported as being conducted the least are privacy risk assessments. These risk assessments would have the best chance of evaluating privacy policies and controls and reducing the frequency of data breaches unintentionally caused by employees.

The 2014 Ponemon report showed that employee negligence is still considered the biggest security risk, with a full 75% of the surveyed organizations reporting it as their largest worry. Companies normally pay very close attention to the process and technological aspects of their information systems, but overlook their own employees as a security factor. In running a business in the health information exchange realm, you cannot call your security preparations done with firewalls and a few privacy and security policy attestation sheets to sign. The more people who are employed in a particular venture, the more variance there will be in education and IT sophistication. Management and employees must be prepared and equipped with the appropriate tools to deal with both known threats and emerging threats. Security built on technology and basic processes are not enough. You must strengthen your weakest link in the security chain by making it clear that all employees have a role to play in information security, and then give them the tools to play those roles.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Enabling the Solutions

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

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. If providers and consumers do not trust an HIE, they simply will not use it -- regardless of how well funded.

Best Practices

A listing of currently accepted best practices would include:

- Common consent and trust agreement forms can offer providers assurance that they are complying with Federal and state requirements, and that their HIE partners are doing the same. In Pennsylvania, Act 121 of 2012 has mandated that the Pennsylvania eHealth Partnership Authority promulgate a common consent form to implement the required “opt-out” consent registry for the state. It also requires the Authority to develop and maintain standards to ensure interoperability (Section 303(a)11). Standardized agreements (DURSA, BAA) and certification standards are being written in a combined effort with stakeholders to implement this interoperability requirement and support the marketplace with common forms.

- 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 sometimes be donated to physicians, enabling wider use of HIE technologies while avoiding prohibitions in the Stark and Anti-Kickback laws. Do enough due diligence to discover how long the accreditation on any given product is guaranteed for, as not all vendors have plans to continuously re-certify.

- View accreditation and certification holistically. Health care providers are subject to a variety of accreditation and certification regimes. 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, regulatory reviews and violation investigations are consistent.

- HITECH allows for a “safe harbor” for breach reporting if the data involved was properly encrypted to NIST standards. This means that public reporting of breached encrypted data is not required. This is the only “safe harbor” exemption for breach notification, and every organization that holds and handles PHI should be implementing it.
Various toolkits exist that contain checklists and outlines for organizations conducting assessments of business practices. While a few are more than 5 years old now (AHRQ, The Health Information Security and Privacy Collaboration Toolkit, 2007), they still contain plenty of information to help with the construction of an internal assessment plan. The basic business advice remains consistent.

**Stakeholder Education**

Informed consumers who trust their privacy will be protected will be willing to enable the benefits of an HIE. Improved and positive patient engagement also will have an impact on medical outcomes. While improving an overall patient experience is often thought of in terms of more time with physicians to ask questions or smoother administrative procedures, the patient or consumer can also be engaged with HIT in positive ways to improve their health care experience.

Some health care entities have made personal health records (PHR) or patient portals available to their patients. Both interfaces are web-based, and allow consumers to interact with some or all of their medical records, and sometimes manage records access consents or send and receive secure email messages to or from their health care providers. Some providers assume the cost of providing these services, as patients appreciate the ability to access their records online, especially if the PHR can be smartphone-based and contain interactive apps. PHRs are also a part of the “Patient Centered Medical Home” model of care concept currently being debated. Of course, all this data living online and meant for consumer-facing access presents a large privacy and security risk to that data, and to the EHR systems that those software applications are connected to.

Patient engagement objectives must also be met to be in compliance with Meaningful Use stage 2 requirements. Health care providers must actively engage patients by providing them with the ability to electronically view, download, and transmit relevant information from their provider’s electronic health records. This could include medication lists, lab results, and discharge instructions. Stage 2 also requires bidirectional secure email with patients – a capacity that is being incorporated into most new EHR products. These requirements facilitate consumer electronic access to their records and providers, while still protecting the privacy and security of that information on the electronic systems and in transit.

Education about consent management is also necessary. Educating patients and caregivers to encourage mutual trust can help eliminate the medical risk inherent in patients who are unwilling to allow the sharing of electronic medical records and caregivers who cannot effectively express the downside to opting-out. Consent management is not a one-size-fits-all topic. Consent management incorporates federal and state legal requirements, patient trust and expectations, technical implementation, and administrative implementation. Some HIOs in Pennsylvania have established opt-in or hybrid models for consent to electronically share medical records between entities. By statute, Pennsylvania was established as an “opt-out” state. This means that a consumer’s records will be shared across the state health information exchange network unless that consumer takes affirmative steps to “opt-out” of that sharing. Patient education about those
choices and their repercussions will be undertaken through consumer brochures and a
standardized opt-out form that will be available online and throughout the state at participating
providers. There is the possibility for marketplace confusion on this topic, as HIOs that do not
chose to participate in the state network may have different consent management tools, forms,
and models. The risk for this consumer confusion through nonparticipation in the state network
and attendant non-standardization of consent forms lies with the HIOs making that business
choice.

Patient and consumer engagement is a hot topic these days, as the public must be accepting of
electronic health information exchange for it to be truly successful. HIMSS has made a Patient
Engagement Toolkit available. The National eHealth Collaborative has created a Patient
Engagement Framework reflecting five stages of engagement (Inform Me, Engage Me,
Empower Me, Partner with Me, Support My eCommunity). The Markle Foundation originally
produced the “Blue Button” concept, which has morphed into a national initiative to promote
access to PHRs. An alphabet soup of federal agencies are participating in the Blue Button
campaign, including the DOD, HHS, and the VA. Online sites that use the Blue Button allow
consumers to download their health data and create medical histories, which can then be shared
with their health care providers. All of these things merge into a national strategy to engage
consumers in their health care by having them actively participate in the capture and use of that
information. The thinking is that more engaged patients with better access to their medical data
will take greater ownership of their health care, and will make better decisions that will
improve medical outcomes.

**Key Technical Properties**

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

- Basic hardware and processes 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 health care IT environment,
  interoperable systems have trust agreements, shared rules for identifying both users and
  patients, shared rules for granting and withholding access, and other technical mitigations
  that ensure the sharing of health care data with strict confidentiality and integrity.

- Scalability – Systems and networks can accept any 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 from, or confuse the primary health care mission.

- Affordability – Privacy and security controls cost less than the total actuarial value of the
  risks they mitigate.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Reasonability – An HIE-scale solution is inappropriate for smaller providers. HIPAA allows scaling of privacy and security mitigations, rather than requiring 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 health care IT products, including their security features. These Connectathons are weeklong interoperability testing events held annually, where systems exchange information with complementary systems from multiple vendors.

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. Following the HIMSS conference, subsets of the vendor participants have repeated their demonstrations at state and regional events.

**Emerging Areas of Risk and New Compliance Challenges**

**Cloud Hosting**

Cloud computing refers to delivering hosted services over the Internet that can be divided broadly into three categories: infrastructure as a service, platform as a service, and software as a service. Cloud services can be public or private or a hybrid of both. Public services are available to any consumer, and private services are data centers or proprietary networks hosted for specific entities. The on-demand nature of these services has made them ripe for adoption and services growth within the health care IT field.

Consumers are already well-used to using cloud services through their smartphones, utilizing online banking, using a personal health record (PHR), or provider-based patient portals. Cloud services have infiltrated the consumer electronics market without the potential patients ever noticing. The federal focus on patient engagement and consumer demand for online access to their medical records will continue to drive this adoption rate. While the market for such services is clear, what are the issues embedded in such growth?

Under the HIPAA Omnibus Rule, cloud hosting services providers are now business associates, and are directly liable for HIPAA compliance. In some cases, tweaking existing contract provisions might be sufficient, but in most cases it would be best if detailed agreements are built from scratch to cover all aspects of these newly characterized relationships. Such service providers, who have not had to absorb that compliance requirement before, might be understandably reluctant to sign such adapted paperwork. Covered entities need to be absolutely sure that all their BAs, including the cloud hosting vendors, are conducting ongoing risk analysis and HIPAA compliance auditing. As cloud hosting services often don’t have a view into the actual data they are hosting due to privacy concerns, negotiating the specifications of such BA agreements can be difficult. Some cloud providers are questioning whether the additional liability and oversight under the Omnibus Final Rule is worth the revenue gleaned from hosting medical data that includes PHI. Some covered entities may take the step of encrypting any data...
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

stored in the cloud to calm fears at both ends of the service agreements about liability for PHI that is lost, stolen, or mishandled.

Every covered entity and business associate that deals with protected health care information (PHI) must comply with the regulations stipulated under the HIPAA act. HIPAA is designed to protect the privacy of patients, and does so by enforcing strict guidelines over how PHI is collected, handled, protected, used, and disclosed.

Although HIPAA does not apply directly to third-party Cloud Service Providers (CSPs), covered entities must require the CSPs to execute contracts (Service Level Agreements (SLAs)) which require them to handle all PHI in compliance with HIPAA guidelines.

When it comes to storing or handling PHI in the cloud in a way that’s HIPAA compliant, there are a few considerations which HIEs should address in a SLA.

- The HIE must ensure that the PHI never leaves the USA. If the PHI is physically moved to another country, it will be out of US legal jurisdiction. Therefore the PHI may be subject to international laws which would force the CSP to invoke actions that would put the HIE out of compliance.

- When PHI is stored in the cloud, the HIE must make sure that it knows exactly where the PHI is physically stored, how many copies exist, whether or not the PHI has been modified, or if the PHI has been breached. Once the HIE turns control over to the CSP, the HIE has no direct control or access to their IT infrastructure. This risk can be mitigated by the utilization of a private cloud environment where the HIE is hosted on dedicated equipment at the CSP location.

- The HIE needs to ensure that the CSP has HIPAA-compliant security measures in place. All servers and storage should be in cages, with redundant power supplies, Disaster Recovery sites, professional security guards, fire suppression systems, etc. The CSP should provide a copy of the SOC2 Annual Audit and HIPAA Certification documents upon request.

- Under the Patriot Act, the federal government may make a request to access PHI which is stored in the CSP’s data center. Additionally, a legal-hold may be served to prevent the CSP from disclosing any PHI breach to the HIE. In this scenario, the HIE would be unable to notify the patient, as required under HIPAA.

- How will the PHI be stored in the CSP’s data center? The HIE may encrypt the PHI before sending it to the CSP. Although this is practical for security purposes, it is not practical for the applications where the PHI must be accessed and manipulated on the CSP server.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Under HIPAA, HIEs are required to provide providers (stakeholders) and patients with the details of their PHI handling practices. However, if this is not specified in the Service Level Agreement, the CSPs may be reluctant to discuss or disclose their internal security policies.

HIPAA Omnibus Rules and the Cloud

The new HIPAA rules under the Omnibus very specifically define cloud service providers (CSPs) as business associates.

“…document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold.”

If a HIE plans to utilize a CSP, there are several planning considerations to keep in mind:

- Select a CSP that offers a HIPAA-compliant environment. The CSP should be able to validate that they have met the HIPAA compliance requirements as defined by the Office for Civil Rights (OCR) through an independent audit.
- The HIE and CSP must execute a Business Associate Agreement, which will ensure that both parties will comply with their side of HIPAA compliance.
- The HIE should ensure that its own infrastructure and that of the CSP interact in harmony from a compliance standpoint.
- The HIE should make sure that the PHI is encrypted, and that it holds and maintains the encryption keys.
- The HIE should insist on a strong Service Level Agreement which contains the terms and conditions necessary to ensure the mitigation of risks associated with HIPAA non-compliance.

Under the Omnibus Rule, the HIPAA “chain of trust” has expanded to include the liability associated with the acts of their respective business associate agents, so the HIE should make sure the business associate agreements are inclusive of all business parties involved.

Cyber Security Insurance and Cyber Attacks

Insurance

In the current environment of evolving technology in the health care realm and the constant threat of costly data breaches, cyber security insurance has become a necessity. For data providers, the public relations black eye doesn't end with the data loss itself, it’s the possible criminal prosecutions, civil penalties and fines, threatened litigation, and the loss of faith amongst the patient population. Specialized insurance products help bridge this gap in risk management and mitigate the monetary damages associated with data breaches, business interruptions, breach notifications, re-marketing, and network damage. As this is a rapidly evolving area, the types of insurance products available to health care organizations can be expected to increase.

Cyber Attacks
The current trends in HIE Cyber Attacks are:

- Increasing sophistication of technology begets easier proliferation of attacks.
- Decreasing cost of technology allows for even the most casual hacker to launch attacks.
- Increasing attack frequency as a result of the above.
- Difficulties in patching systems where the customer and virus protection vendor are not able to stay current with the evolving types of virus, malware, etc.
- Increasing network connections, dependencies, and trust relationships propagates the vulnerability points susceptible to attacks.

These trends have resulted in the following concerns:

- Medical Devices/Robotic Surgery are Wi-Fi connected
- Impact of Mobile Devices - BYOD
- Internal & External Breaches
- Data Leakage – the trickle of PHI under breach
- Limits of Technology & Inadequate Security Systems
- Funding for security tools
- Patient’s Lack of Confidence in the privacy and security of their data
- Third Parties-Vendors are now covered entities, but are they ready for HIPAA compliance
- Remote Connections via the rising mHealth environment

The Concepts of Information Assurance (CIA), represents the gold standard and should be addressed by the HIE

- Confidentiality (privacy)
- Integrity (quality, accuracy, relevance)
- Availability (accessibility)

ONC Cyber Security Guidelines

- The new privacy and security guidelines--aimed at protecting the vast amount of health care information transmitted by state Health Information Exchanges--are now in place.
- HIEs are networks intended to help states manage the electronic exchange of health information among health care providers and hospitals within their states and across state lines.
• Privacy and security policies are required as a condition of accepting part of the $550 million federal grant money funding the development of state-based HIEs.

“The guidelines, issued by the Office of the National Coordinator for Health IT (ONC), provide a common set of rules of the road designed to build confidence in the system on both the provider and patient level”........ ONC

• Under the new guidelines, state HIE grantees are required to develop privacy and security policies to address each of the fair information practice principles as outlined by ONC.
  
  o The principles include individual access to information; the right to correct errors; openness and transparency; collection, use and disclosure limitations; security safeguards; data quality and integrity; individual choice; and accountability.

• The ONC also noted that there was no "one size fits all" approach when developing privacy and security policies for HIEs.
  
  – For example, some state HIEs merely serve as information conduits, ensuring the secure exchange of identifiable health information among health care providers, without accessing or storing any of that data. This type of HIE doesn't have to worry about data quality or providing individuals access to copies of their health information or to have errors corrected or noted.
  
  – However, state HIEs that "store, assemble, or aggregate" identifiable health information are required to develop policies to address all of the fair information practices, including data quality, individual access and the right to correct errors.

• If an HIE's current privacy and security policies don't comply with the new ONC requirements and guidance, they have to be rewritten and a timeline for making those changes given to the ONC.

• The new requirements are consistent with the recommendations developed and issued by the Privacy and Security Tiger Team of the Federal Health IT Policy Committee.

HIE Privacy & Security Policies

• All of the information that passes through the HIE is password protected and encrypted at its source using state of the art tools to protect the transmission and security of the data.

• Access to the network is monitored and restricted to only those qualified medical professionals who have demonstrated a need to know the requested information.
HIE Security Architecture

- The secure exchange of electronic health information is important to the development of electronic health records (EHRs) and to the improvement of the U.S. health care system.
- While the U.S. health care system is widely recognized as one of the most clinically advanced in the world, costs continue to rise, and often preventable medical errors occur.
- Health information technology (HIT), especially the development of electronic health records for use in both inpatient and ambulatory care settings, has the potential for providing reliable access to health information and thereby improving the health care system. However, the prospect of storing, moving, and sharing health information in electronic formats raises new challenges on how to ensure that the data is adequately protected.

NwHIN and HealtheWay Security Architecture

- Protecting electronic patient health information is crucial to developing systems and structures that support the exchange of that information among health care providers, payers, and consumers using Health Information Exchanges (HIEs).
- As noted in the Summary of the Nationwide Health Information Network (NwHIN) report from the Office of the National Coordinator, "An important core competency of the HIE is to maintain a trusting and supportive relationship with the organizations that provide data to, and retrieve data from, one another through the HIE. The trust requirement is met through a combination of legal agreements, advocacy, and technology for ensuring meaningful information interchange in a way that has appropriate protections."

NIST Security Architecture

- NIST published "Security Architecture Design Process for Health Information Exchanges (HIEs) (NISTIR 7497)" in September 2010, to provide a systematic approach to designing a technical security architecture for the exchange of health information that leverages common government and commercial practices and that demonstrates how these practices can be applied to the development of HIEs.
- The publication assists organizations in ensuring that data protection is adequately addressed throughout the system development life cycle, and that these data protection mechanisms are applied when the organization develops technologies that enable the exchange of health information.

The operating model outlined in the NIST publication will help organizations that are implementing HIEs to:

- Understand major regulations and business drivers.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- Identify cross-organizational enabling services.
- Define supporting business processes (for each service).
- Develop notional architectures (as a blueprint to support services, processes, and the selection of technical solutions).
- Select technical solutions.

FDA Cyber Security Recommendations for HIEs

- Restricting unauthorized access to the network and networked medical devices.
- Making certain appropriate antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
- Developing and evaluating strategies to maintain critical functionality during adverse conditions.

Cyber Security Best Practices

- Implement best Practices for Technology Environment
  - Configuration Management
  - Software Maintenance
  - Operating Maintenance
- Mobile Device Management (BYOD) infrastructure in place
- Establish a Security Culture via awareness and education
- Provide for backup and disaster recovery for PHI
- Monitor checklists and IT Service/Change Management for all Elements, Passwords & Strong Authentication
- Implement Anti-Virus Software – and stay current
- Keep Firewall(s) up to date and robust enough
- Govern controlled access to PHI – provisioning of authorized access
- Controlled Physical Access via state of the art data centers
- Limit Network Access reduce random, unauthorized access, perform penetration testing and annual audits
- Plan for the Unexpected – in an ever changing technology and clinical practice environment

Mobile Device Management (BYOD)

BYOD or “bring your own device” is becoming commonplace all across the health care spectrum as the majority of professionals bring their personal mobile phones to work and use
them there. Some workplaces have even allowed employees to bring their own devices to be used at work and then pay part of the resulting connectivity bill. This saves the business the cost and maintenance of the devices, and effectively makes the employees available 24/7. Thus, BYOD can be seen as creating efficiencies, but it carries with it its own risks.

Deploying BYOD in a health care setting means having policies and procedures in place to help manage and mitigate the privacy and security issues this consolidation of personal and business devices produces. Your IT department will be facing:

- Problems related to deploying appropriate mobile security solutions. In an environment where personal devices can be of a myriad of types, brands, age, and power, it will be a challenge to ensure that unified threat management software is installed properly and used appropriately. Such coordination will be necessary particularly where providers could be accessing data that is covered by HIPAA from a personal device. This will require ongoing training as to policies covering such software, and the ability to identify noncompliant people and devices.

- Networks must be powerful enough to support all internal technology plus all personal technology without causing network slowdowns or failures. This might require network upgrading to support BYOD solutions. A facility’s wireless network will be particularly strained by the addition of perhaps thousands of additional devices.

- Whose problem is a lost device? A lost device that perhaps contains an account to access PHI and can be easily used on a particular secure network is a security issue for both the device owner and their employer. Training as to properly physically securing such devices and keeping their enterprise-related security up to date is crucial. A majority of breaches reported to HHS are due to the loss or theft of mobile devices. Employees in a BYOD environment must be contractually required to turn over devices for security audits and investigations, and must be trained to report a lost device promptly. The challenge for the employer will be balancing these appropriate security measures with employee privacy in a noninvasive manner.

- The expanded penalties for data breaches under HITECH and the Omnibus. BYOD can greatly expand a facility’s exposure to the risk of a data breach by exponentially expanding the number of devices that can access and contain PHI, and allowing the transportation of those devices out into the environment away from the standard internal controls. This risk must be balanced against the perceived benefits of such a program.

HIMSS and mHIMSS have published a white paper focused on security, *Security of Mobile Computing Devices in the Health Care Environment*. The paper contains a list of questions that health care organizations should ask themselves before deciding to deploy a BYOD program.

A recent survey showed that 81 percent of providers allow their employees to use their own iPads, smartphones and other mobile devices in workplaces. Of those employees, half access PHI. On the flip-side, about half of the organizations have implemented mobility device
management to secure employee-owned mobile devices, and the rest showed little confidence that the BYOD access is secure.

HIPAA and state laws put strict safeguards around the management of PHI. With the Office of Civil Rights stepping up their enforcement, HIEs should implement the most comprehensive privacy and security policies/practices that the system can bear, including those that cover the use of BYOD.

The best policies are based on the HIE’s commitment to protecting patients’ sensitive information. Demonstrating good intentions and strong policies are the best way to achieve compliance in an era of tightening regulations and increasing use of BYOD in health care.

**Physician and Patient Portals**

Stage 2 of the Meaningful Use requirements promotes the use of patient portals that allow patients to view their records, download copies of records, transmit their records, and to send secure messages to their health care provider. This requirement is to support the broader cause of effective patient engagement and to give patient’s more control over their health information. This MU2 aspect has sparked the patient portal market, and has gotten health care entities thinking about how to integrate such technology into their security landscape.

Patient portals are being built in a variety of flavors. Very basic portals can be accessed only from inside an HIOs architecture, or may be public-facing but only allow very basic functions such as bill paying, refill requests, and appointment scheduling. Such portals do not fulfill the MU2 requirements and trigger incentives if they do not register a certain level of patient engagement and use.

Effective patient portals must have a high usability factor, must support fast and easy communication, and must be reliable and secure on all the major platforms. A portal that is difficult to use or technologically unstable could go unused, tarnishing your brand and wasting your technology dollars.

Portals come with their own distinct technology challenges. There is a balance to be struck as to strong passwords versus passwords so complex that patients can’t remember them or effectively use them. Consumer-facing portals must also have protocols in place for both identification proofing and account provisioning. This might require the assignment of additional staff for account management and tech support. HIPAA also requires that patients have an effective route to request corrections to their records, and while this is another task it makes sense to roll into a portal, there must be protocols in place as to how to respond to such requests.

While health care entities may believe that after granting access to a patient to see their own records, their work is done, this is not true. Organizations choosing to provide such portals are not out of the equation simply because what happens to the records after a patient acquires them is not a HIPAA concern. The implementation of portals brings the HIE to a more personal relationship between the physician and patient. Merriam-Webster defines portal as: “A site
serving as a guide or point of entry to the World Wide Web [HIE] and usually including a search engine or a collection of links to other sites arranged especially by topic.” This point of entry can be both a relationship builder and a security weakness. A patient-facing portal is a possible gateway to the organization’s medical record repository, and as such, could become a target for hackers, making penetration testing essential.

How do HIEs and portals inter-relate? Physicians will have the ability to access a local and/or regional HIE’s physician portals to view a specific patient’s treatment history, providing valuable health data that may be useful prior to treatment. Patients will link via portals to the repository of a HIE. In the future, the patient’s continuum health record – agnostic as to where the care was provided – will be viewable in a patient portal. Patients will have the ability to correct errors in their EMR if they exist, and be reminded of previous care they have received and their future care events.

Patient-facing portals may also allow the providers to operationalize and absorb patient-generated health data (PGHD). PGHD are health-related data created and recorded by the patient on their own behalf, and then submitted to a general health record repository. This can be through a patient-centric portal, a PHR that the provider receives information from, or through medical mobile apps. PGHD can include health history information, treatment history information, biometric data like blood glucose readings, symptoms, and lifestyle choices (smoking, alcohol consumption). This means there must be policies in place as to the possible incorporation of such self-reported data into the general health record, and there may be consent management issues as to whether the patients will consent to having such information incorporated or shared beyond the targeted physician. So, while such data can possibly fill in gaps in the existing clinical data and provide an ongoing health picture rather than from only clinical visit points in time, providers will need to evaluate how to handle such records and whether to use the data as part of a care plan. When collecting such data through a portal, patient access to the internet and appropriate access technology, usability of the portal, general health literacy, and other such factors may be barriers to PGHD use by patients and acceptance by providers.

ONC has identified PGHD as important for advancing patient engagement. In April 2012, ONC commissioned a white paper on the topic. Various Federal advisory Committees are considering recommendations about the inclusion of PGHD in Stage 3 Meaningful Use. In December 2013, ONC released an issue brief on the work so far, including the recommendations from consulted workgroups. In general, ONC believes PGHD will be an important tool to empower patients, and as such deserves further study.

The HIE portal is an access point for both patients and physicians that provides a convenient platform to communicate real-time through various venues, which may differ among portals. Some HIE portals allow only basic interchange of data in the form of scheduling or rescheduling appointments, requesting a prescription refill and filling out paperwork prior to their next appointment. Other, more robust HIE patient portals – especially those built to meet MU2 requirements - will allow patients to access clinical care documents and support electronic viewing of their clinical results. Future portals will give the physician better access to the
patient’s record, with the ability to send email reminders regarding future visits or reference online information about valuable health resources for specific diseases.

HIE Portals directly connect the patients to their care program across the spectrum, thus fulfilling the potential to directly connect patients to their care programs.

**Checkbox Compliance**

In today’s environment of what is perceived as overwhelming regulatory control, many organizations address compliance as a temporary project where the goal is to get the auditor to check the appropriate box. This attitude results in very inefficient approaches to compliance initiatives. Achieving a level of compliance that can be visualized as a neatly checked-off list may be an organizational requirement, but it is not a guarantee that your procedures and policies are effective and your systems and data will be secure. Compliance initiatives should be the catalysts that continuously test and evolve your security and controls. The neatly checked-off list does not constitute compliance without the related security due diligence. Security is not a once a year audit issue, it must be integrated into the daily workflow of the organization at all levels.

**Convergence of HIOs and Social Media**

Social media presents health care providers with many opportunities for patient engagement. With this opportunity, however, come many privacy and security issues that must be weighed and addressed.

In general, social media are the online tools and platforms that allow the sharing of information through conversation and communication. Facebook and Twitter are the most commonly recognized and used social media platforms. Organizations have adopted these tools for brand education and marketing purposes, to engage consumers in conversations, or to manage customer communications. Health care organizations engage with social media through writing and sponsoring blogs, creating profiles and communities of interest on Facebook and Google+, communicating short messages through “tweets”, posting video content to YouTube, creating podcasts, and establishing Wiki websites. Many health care startups and software vendors are adopting “gamification” as a user engagement and adoption tool; leveraging people’s natural competitive urges through social media to achieve a stated wellness goal or accumulate intangible points as rewards toward a goal.

The ready availability of electronic medical records on some of the same systems and devices that can connect to and use social media poses various challenges to the health care community that wishes to utilize these engagement tools. Individuals have been empowered to network and communicate, but the danger lies in treating the Internet as a whole as equal in communication value. Once information is released via social media, it is released to an entire set of connected entities, many of which will be personally unknown to the consumer originating the message, file, or picture. This is in stark opposition to when a person sends an email message, as that would go only to the people listed as recipients. In social media environments, everyone can see the content, whether it pertains to them or not. This is called “data leakage”. Employees can
inadvertently or purposely leak patient or company information on social media that may increase general liability exposure or directly violate HIPAA.

Social media tools have a tendency to distance people from their legal responsibilities, leaving them to their own judgment as to their actions. How can a health care entity manage the risk connected to these tools while still allowing their use in work spaces and promoting their usefulness in their business model?

Health care entities need to develop a social media policy that covers both how the organization plans on leveraging social media for business purposes, and a behavioral policy that states the expectations of how employees may conduct themselves on social media. The policy covering private employee conduct must be respectful of concerns about public forums and constitutional speech protections, while emphasizing the required protections of patient privacy and PHI.

Social media is here to stay, and so are both the risks and the benefits. The risks fall into categories governed by human behavior, and that risk inherent in the technology. Social media sites are now so large and pervasive it is almost impossible for those site managers to prevent the periodic introduction of malicious code and links. Infections that originate from social media, especially on devices in a BYOD enterprise environment, pose an ongoing risk to data and systems. Organizations that have made the decision to be active on social media need to have good policies in place, and to actively perform social media risk assessments and internal trainings that are part of an overarching strategy that has been harmonized with organizational goals.

**Disposal of PHI**

The HIPAA Privacy and Security Rules require that covered entities have all appropriate safeguards in place to protect PHI, which includes the appropriate disposal of such PHI. The Rules do not specify required methods for this disposal, leaving the individual health care organizations to assess any relevant privacy implications attached to the method of disposal being considered. Paper-based PHI can be shredded, burned, pulped or otherwise rendered unreadable and unreconstructable. Electronic PHI can be cleared (overwritten), purged (degauussed), or otherwise disintegrated or destroyed. Other types of portable PHI (prescription bottles) can be stored for destruction in opaque bags. Many covered entities employ specialty vendor business associates to help with such secure bulk destruction.

In 2009, CVS Caremark agreed to settle FTC and HHS charges for $2.25 million that it had been improperly throwing trash containing PHI into open dumpsters that were accessible by the general public and was not training employees as to the appropriate disposal of material containing PHI. CVS was directed to cease these practices and train their employees immediately. This is the type of improper disposal of PHI that comes to mind when most people think about this topic – along with media stories that pop up about computers mistakenly recycled or sold that still contained unscrubbed PHI. There are, however, more technical issues that relate to how information is moved between servers and computers within a health information exchange organization, and how that information is archived or disposed of. This is also a factor in HIPAA required contingency planning, as organizations must explain in their
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

plans how health care data is to be moved without violating HIPAA privacy and security requirements.

**PHI Ownership and Proprietary EHRs/HIEs**

If you choose to end your contract with an EHR and/or HIE vendor, who owns that data? In 2013, the Milwaukee Health Services (MHS) ended a contract with an EHR vendor on bad terms. MHS claimed that the EHR system was never functional, and a great deal of extra money was spent to fix the system to no avail. The EHR vendor claimed that MHS owed them money, and until the bill was paid, MHS could not access or transfer any of the 40,000 patient records that were stored in a proprietary format. The contract dispute wound up in court, with the records as the disputed prize. Most health care providers would believe that they owned their patient’s data, regardless of the format, and that the patient’s also had a privacy and ownership interest in that information. They would also think that any other entity withholding that data would be violating many laws requiring that health care entities release patient records upon request. They would not think that such issues are for a court to decide while records access is denied by a vendor. They would be wrong on both counts.

How can HIEs and health care providers avoid this sort of denial-of-records dispute? Contract negotiation is key to avoiding this issue. As the EHR marketplace contracts, more and more records will be placed in the hands of fewer vendors with more market power. Older EHR systems are being replaced to make way for interoperable MU2 compliant EHR systems where the vendor hosts the application in the cloud. This leads to old electronic records being gradually converted to a new proprietary format, something which then may require the cooperation of two or more vendors.

Contract provisions that would have been helpful to the providers in this case would have been:

- Mediation and/or arbitration requirements,
- penalties or liquidated damages for delays in releasing records in the event of contract failure or non-extension,
- strong contractual warranties and indemnities,
- and a reasonable designated judicial venue.

**Business Intelligence and Data Analytics**

Big data and data mining are two phrases that have become part of the general zeitgeist in the last few years. Internet privacy advocates have expressed fears about the rise of health information exchange leading to the extensive mining of aggregated medical records for both the marketing of products and services to patients and the actual marketing of patient data itself. As information technology grows and evolves in the health care arena, enormous volumes of data will be produced. The issue for organizations is not only how to use this data while remaining legally compliant, but how to handle the data ethically so as to retain the trust of their patients and the public at large.
The doctor-patient relationship is dependent on high levels of trust. If patients do not trust their doctor or the HIO the doctor is a member of to protect the confidentiality of their medical information, then they may withhold information or ask that certain information not be recorded in their records. Concerns about the harm inherent in the release of sensitive personal information have resulted in the HIPAA Privacy Rule and various other state and federal laws. None of these laws actually forbid data mining or business analytics, but they do require that the privacy and security of the information be respected.

De-identified data has been routinely used to compile information into aggregate forms that do not include what the law terms “unique identifiers” (patient name, address, phone number, social security number (SSN)) that then is released or used for research or industry analysis. This used to be sufficient to protect identities of the patients who have contributed to the databases. The evolution in software and technology, however, has outstripped these standards and now can be used to associate such de-identified data against public databases, essentially “re-identifying” it. Any business that is using patient data for analysis, regardless of the intent, must be very sure to stay within the ethical standards outlined in HIPAA and the Omnibus Final Rule to avoid legal liability and penalties.

Many HIE organizations are recognizing the need to add data analytic/BI capabilities to their data exchange functions. Analytics includes the processes of inspecting, cleaning, transforming and modeling data to extract and report useful information, suggest predictive conclusions and support real-time decision-making. These processes encompass both diverse software and techniques. The utilization of analytics represents a natural extension of the inherent capabilities that a HIE can provide to its stakeholders. The data contained within a HIE needs to be used in a meaningful manner to benefit the care givers and patients in their daily lives, support the business model, and still respect all of the appropriate privacy regulations.

Backup and Disaster Recovery for HIOs

While it is normal for HIOs/HIEs to do some planning for the backup of their data and systems in the event of an emergency, full scale disaster recovery planning and implementation is rare. It’s important for health care executives to make the business case within their organizations so that appropriate budgeting for a disaster recovery plan is delineated. A HIPAA covered entity must have both a contingency disaster or emergency plan to ensure continued access to PHI in the event of a system failure, and a data backup plan. This Contingency Plan standard is part of the administrative safeguards delineated by the HIPAA Security Rule.

It is possible for such emergency plans to include the establishment of a virtual data access system. While this virtualization can be very useful to effected organizations, health care organizations must still maintain HIPAA compliance.

If the HIO/HIE has their data infrastructure hosted offsite with a cloud service provider (hopefully in a location with a low risk of natural disasters), then the contingency plans may need to contain downtime procedures to revert back to paper/manual processes. If the data infrastructure is hosted onsite, then the disaster recovery plan will need to be robust enough to cover both business contingency planning and full scale backup and disaster recovery of the
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

internal technology and PHI. HIOs/HIEs should require fully redundant IT infrastructure, inclusive of servers, network capability plans, and simultaneous data mirroring. This can be achieved through cloud hosting and backup, with the result that onsite power, connectivity, and network capability will become the most immediate needs. The backup and hosting locations should be separate geographical locations to guard against the loss of both in an offsite natural disaster.

Planning is essential to the production and success of all such backup, contingency, and recovery plans. This may sound obvious, but it is actually where most unprepared organizations failed in their processes. Many organizations believe such planning is either unnecessary or too costly. Protecting health care (PHI) data and ensuring it will be available when needed means putting funding, procedures and plans in place to mitigate disasters. While this is about analyzing the impact of a business interruption on revenue, it is also about making critical health information available in the time of a disaster, while subsequently achieving HIPAA compliance.

Addressing Barriers to Solutions

The Pennsylvania HIT marketplace faces a number of unique challenges. As the Commonwealth has taken the step of having the designated governance entity, the Pennsylvania eHealth Partnership Authority, preside over a federated system using a “network of networks” architecture approach, interoperability and standardization are both challenges and the keys to success.

Act 121 of 2012 was passed unanimously by both chambers of the Pennsylvania General Assembly, and then signed into law by Governor Corbett on 7/5/12. This Act is the founding legislation for the Pennsylvania eHealth Partnership Authority (the Authority). The Act establishes the Authority as the governing body for HIE interoperability within the Commonwealth of Pennsylvania.

The Authority is an independent agency, with an associated Board of Directors, that has been tasked with establishing an opt-out registry and a provider directory that will serve as the source of truth for the entire state’s HIE community.

Patient education materials and related tools for the stakeholder community will be developed and distributed to achieve awareness and support for HIE in Pennsylvania. The Authority will exist as an independent agency for five years, before being reviewed in its final year (2017) for continued independence, transition to a nonprofit, or being sunset.

The Authority’s policy and procedures framework incorporates the eight Privacy and Security Principles of the S&I Framework to define and create the policies and procedures required to protect the exchange of electronic PHI. For each policy developed, staff followed a standardized process to outline and draft the policy and to share the document with stakeholders. Staff and stakeholders gathered sample policies from stakeholders, Commonwealth agencies, Federal sources, and other marketplace sources, which were updated and evolved as needed, consistent with federal and state legal requirements. The goal is to establish policies for the network being built that all participants will be able to use as a policy resource in the exchange of PHI.
network is a federated model, a “network of networks” connecting both larger and smaller HIOs to each other for the benefit of all Pennsylvanians, where all participants continue to maintain their own information, and where no patient’s clinical information is centrally stored.

Pennsylvania has adopted an HIE model that considers the needs of stakeholders, communities and Commonwealth agencies, and achieved stakeholder support to enable the use of HIT and advance HIE. The Authority’s mission is to develop, establish, and maintain a health information exchange that complies with federal and state law and that promotes efficient and effective communication among multiple health care providers and payers. It is hoped that the existence of this dedicated agency will help to ease some of the barriers to solutions for the various health care entities in Pennsylvania participating in health information exchange, and ultimately help to improve the health and care of all Pennsylvanians.
References

Breaches Affecting 500 or More Individuals
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Cybersecurity Insurance Workshop Report

Fourth Annual Study on Patient Privacy and Data Security, Ponemon Institute

Guide to Privacy and Security of Health Information, The Office of the National Coordinator for HIT, ver 1.2, June 2012,

Health IT Privacy & Security Resources
http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

HIMSS Patient Engagement Toolkit

HIMSS paper, Security of Mobile Computing Devices in the Healthcare Environment

HIMSS Social Media in Healthcare: Privacy and Security Considerations

HIPAA Omnibus Final Rule

HITECH Act

How To Avoid Denial-of-Access Disputes with EHR Vendors

Markle Common Framework for Private and Secure Health Information Exchange,
http://www.markle.org/health/markle-common-framework/connecting-professionals

National eHealth Collaborative Patient Engagement Framework
http://www.nationalehealth.org/patient-engagement-framework

ONC Help on Mobile Device Security

PAeHI White Papers
Patient-Generated Health Data and Health IT, Issue Brief
http://www.healthit.gov/sites/default/files/pghd_brief_final122013.pdf

Patient-Generated Health Data, White Paper

HHS Security Risk Assessment Tool

The Privacy and Security Gaps in Health Information Exchange

U.S. Department of Health and Human Services, FAQ About Disposal of PHI
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfqs.pdf
Appendices

1) Sample DURSA, federal DURSA adopted 2011, used by HealtheWay, Inc.


Supporting DURSA policy document.


2) Sample BAA


3) Opt-Out form for Pennsylvania

http://www.paehealth.org/

4) PAeHI 5/14/14 Summit Slide Deck, “Ensuring Privacy and Security of Health Information Exchange in Pennsylvania”.

http://www.paehi.org/_files/live/PAeHI_P_S_Presentation_Slides_Final.pdf
Restatement I of the Data Use and Reciprocal Support Agreement (DURSA)

Version Date: May 3, 2011
Overview

Introduction

In 2008, as part of the Nationwide Health Information Network Phase II Trial Implementations, a multi-disciplinary team was assembled to develop a comprehensive agreement that would create a legal framework using existing law for the electronic exchange of health data. This agreement, called the Data Use and Reciprocal Support Agreement or DURSA, was first executed by a number of Federal agencies and non-Federal organizations (the “Participants”) beginning in November 2009.

The executed DURSA contains a provision describing the creation of a Coordinating Committee that is charged with maintaining and evolving this Agreement. Pursuant to that charge, in 2010, the Coordinating Committee established a Task Group to suggest revisions to the Agreement based on the experience gained with the early implementations and to accommodate new opportunities for the promotion and expansion of health information exchange.

This Overview was prepared to facilitate the reader’s understanding of the DURSA, and to place the DURSA into an appropriate context.

Why is a Data Use and Reciprocal Support Agreement (DURSA) Needed?

The DURSA is a legal agreement created to promote and establish trust among the Participants. It codifies a common set of trust expectations into an enforceable legal framework, and eliminates the need for point-to-point agreements.

What is the Data Use and Reciprocal Support Agreement (DURSA)?

The DURSA is the legal, multi-party trust agreement that is entered into voluntarily by all entities, organizations and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services and policies developed in coordination with the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services. (Those who sign the DURSA are known as "Participants.")

The DURSA builds upon the various legal requirements that Participants are already subject to and describes the mutual responsibilities, obligations and expectations of all Participants under the Agreement. All of these responsibilities, obligations and expectations create a framework for safe and secure health information exchange, and are designed to promote trust among Participants and protect the privacy, confidentiality and security of the health data that is shared.

The DURSA is based upon the existing body of law (Federal, state, local) applicable to the privacy and security of health information and is supportive of the current policy framework for
health information exchange. The DURSA is intended to be a legally enforceable contract that represents a framework for broad-based information exchange among a set of trusted entities. The Agreement reflects consensus among the state-level, federal and private entities who were involved in the development of the DURSA regarding the following issues:

- Multi-Party Agreement
- Participants Actively Engaged in Health Information Exchange
- Privacy and Security Obligations
- Requests for Information Based on a Permitted Purpose
- Duty to Respond
- Future Use of Data Received from Another Participant
- Respective Duties of Submitting and Receiving Participants
- Autonomy Principle for Access
- Use of Authorizations to Support Requests for Data
- Participant Breach Notification
- Mandatory Non-Binding Dispute Resolution
- Allocation of Liability Risk

**Will the DURSA continue to evolve?**

Yes. An initial group of Participants executed the DURSA in 2009 to support the first set of electronic health information exchange activities in production under the Agreement. Since then, other entities wishing to transact health information electronically using the agreed upon standards, services and policies have executed the DURSA. Additional entities are expected to execute the Agreement over time. As a living document, the DURSA is being maintained using the process described in the Agreement. An amended and restated version of the DURSA will be available for execution in 2011.

When the Department of Health and Human Services issues final regulations addressing governance of the nationwide health information network, the Coordinating Committee will likely convene another Task Group to assess how the DURSA might need to be revised to accommodate the new regulations.

**Can the DURSA be Used for Other Purposes?**

The DURSA was developed for a specific purpose – to establish the legal framework and to support the trust framework for health information exchange using an agreed upon set of standards, services and policies. Others may find this document helpful or informative for other purposes, for instance, when addressing practical issues related to other types of information exchange models. The DURSA is not intended to be used, however, for other purposes outside of the purpose for which it has been created. As a result, entities interested in using this Agreement for other information exchange purposes are encouraged to seek their own legal counsel regarding the applicability and appropriateness of the DURSA to other settings.
Data Use and Reciprocal Support Agreement

This Restatement I of the Data Use and Reciprocal Support Agreement (“DURSA” or the “Agreement”) is made and entered into by and between the undersigned (hereinafter referred to individually as “Participant” and collectively as “Participants”) as of the Effective Date.

WITNESSETH:

WHEREAS, the Participants who previously have executed the Data Use and Reciprocal Support Agreement dated November 18, 2009, desire to amend and restate the Agreement in its entirety in order to accommodate developments that have occurred since then for the promotion and expansion of health information exchange;

WHEREAS, the Participants desire to electronically Transact, on their own behalf or on behalf of their Participant Users, health information among Participants using the Performance and Service Specifications;

WHEREAS, the Participants recognize that the Office of the National Coordinator for Health Information Technology (“ONC”) plans to conduct rule-making to establish a governance mechanism for the Network. This Agreement is not intended to preempt in any manner or presume any part of that rule-making process. Rather, the Participants enter into this Agreement to enable their voluntary participation in health information exchange activities, as set forth below;

WHEREAS, the Participants are organizations that oversee and conduct, on their own behalf and/or on behalf of their Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations; have the technical ability to meet the Performance and Service Specifications to electronically transact health information on their own behalf or on behalf of their Participant Users; have the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require their Participant Users to comply with applicable requirements in this Agreement; and have each individually been accepted by the Coordinating Committee as a Participant;

WHEREAS, the relationship between the Participant and the individuals whose records are available within or through their respective Systems varies from Participant to Participant and, in some cases, there is no relationship at all;

WHEREAS, as a condition of Transacting information with other Participants, each Participant must enter into this Data Use and Reciprocal Support Agreement and has agreed to do so by executing this Agreement or the Joinder Agreement;

NOW, THEREFORE, for and in consideration of the mutual covenants herein contained, the Participants hereto mutually agree as follows:
1. **Definitions.** For the purposes of this Agreement, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout this Agreement.

   a. **Applicable Law** shall mean: (i) for the Participants that are not Federal Participants, all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements; (ii) for the Federal Participants, all applicable Federal statutes, regulations, standards and policy requirements.

   b. **Authorization** shall have the meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and include any similar but additional requirements under Applicable Law.

   c. **Breach** shall mean the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting such Message Content pursuant to this Agreement. The term “Breach” does not include the following:

      (i) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User if—

      (I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and

      (II) such Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or

      (ii) any acquisition, access, disclosure or use of information contained in or available through the Participant’s System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

   d. **Business Associate** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

   e. **Common Participant Resources** shall mean software, utilities and automated tools made available for use in connection with the Transaction of Message Content pursuant to this Agreement and which have been designated as "Common Participant Resources" by the Coordinating Committee pursuant to the Operating Policies and Procedures.

   f. **Confidential Participant Information,** for the purposes of this Agreement, shall mean proprietary or confidential materials or information of a Discloser in any medium or format that a Discloser labels as such upon disclosure. Confidential Participant Information includes, but is not limited to: (i) the Discloser’s designs, drawings, procedures, trade secrets, processes, specifications, source code, System architecture, security measures, research and development, including, but not limited to, research protocols and findings,
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

passwords and identifiers, new products, and marketing plans; (ii) proprietary financial and business information of a Discloser; and (iii) information or reports provided by a Discloser to a Receiving Party pursuant to this Agreement. Notwithstanding any label to the contrary, Confidential Participant Information does not include Message Content; any information which is or becomes known publicly through no fault of a Receiving Party; is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from a Discloser as documented by Receiving Party’s written records; or, is independently developed by Receiving Party without reference to, reliance on, or use of, Discloser’s Confidential Participant Information. Message Content is excluded from the definition of Confidential Participant Information because other provisions of the DURSA address the appropriate protections for Message Content.

g. **Covered Entity** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

h. **Digital Credentials** shall mean a mechanism that enables Participants to electronically prove their identity and their right to Transact Message Content with other Participants.

i. **Discloser** shall mean a Participant that discloses Confidential Participant Information to a Receiving Party.

j. **Dispute** shall mean any controversy, dispute, or disagreement arising out of or relating to this Agreement.

k. **Dispute Resolution Subcommittee** shall mean the standing subcommittee of the Coordinating Committee that is established pursuant to, and performs the tasks described in, Attachment 6 of this Agreement.

l. **Effective Date** shall mean the date specified in Section 23.12 of this Agreement.

m. **Emergent Specifications** shall mean the technical specifications that a group of existing and/or potential Participants are prepared to implement to test the feasibility of the specifications, to identify whether the specifications reflect an appropriate capability for the Participants, and assess whether the specifications are sufficiently mature to add as a production capability that is available to the Participants.

n. **Federal Participants** shall mean those Participants that are Federal agencies.

o. **Governmental Participants** shall mean collectively those Participants that are local, state or Federal agencies.

p. **Health Care Operations** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

q. **Health Care Provider** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

r. **Health Information Service Provider or HSP** shall mean a company or other organization that will support one or more Participants by providing them with operational, technical, or health information exchange services.

s. **Health Plan** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Regulations.

**t. HIPAA Regulations** shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect on the Effective Date of this Agreement and as may be amended, modified, or renumbered.

**u. Joinder Agreement** shall mean the agreement that each New Participant signs pursuant to which the New Participant agrees to be bound by this Agreement. The form of the Joinder Agreement is attached hereto as Attachment 7.

**v. Message** shall mean an electronic transmission of Message Content Transacted between Participants using the Specifications. Messages are intended to include all types of electronic transactions as specified in the Performance and Service Specifications, including the data or records transmitted with those transactions.

**w. Message Content** shall mean that information contained within a Message or accompanying a Message using the Specifications. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, Digital Credentials, and schema.

**x. Network** shall mean the all of the standards, services and policies identified by ONC that enables secure health information exchange over the Internet. As of December 2010, the group of ONC identified standards, services and policies is called the Nationwide Health Information Network, but may be renamed by ONC.

**y. New Participant** shall mean an organization or agency that is approved as a Participant by the Coordinating Committee pursuant to the Operating Policies and Procedures and Section 23.03 of this Agreement.

**z. Non-Federal Participants** shall mean collectively those Participants which are not Federal Participants.

**aa. Non-Governmental Participants** shall mean collectively those Participants which are not Governmental Participants.
bb. **Notice or Notification** shall mean a written communication, unless otherwise specified in this Agreement, sent to the appropriate Participant’s representative at the address listed in Attachment 4 or the Coordinating Committee in accordance with Section 22.

c. **ONC** shall mean the Office of the National Coordinator for Health Information Technology in the Office of the Secretary, U.S. Department of Health and Human Services.

dd. **Operating Policies and Procedures** shall mean the policies and procedures adopted by the Coordinating Committee that describe (i) management, operation and maintenance of the Performance and Service Specifications; (ii) qualifications, requirements and activities of Participants when Transacting Message Content with other Participants; and (iii) support of the Participants who wish to Transact Message Content with other Participants. The Operating Policies and Procedures are attached hereto as Attachment 3, as amended from time to time in accordance with Section 11.03.

e. **Participant** shall mean any organization that (i) meets the requirements for participation as contained in the Operating Policies and Procedures; (ii) is provided with Digital Credentials; and (iii) is a signatory to this Agreement or a Joinder Agreement. Participants may act as either a Submitter, Recipient or both when Transacting Message Content.

ff. **Participant Access Policies** shall mean those policies and procedures of a Participant that govern the Participant Users’ ability to transact information using the Participant’s system including, but not limited to, the Transaction of Message Content.

gg. **Participant User** shall mean any person who has been authorized to Transact Message Content through the respective Participant’s System in a manner defined by the respective Participant. “Participant Users” may include, but are not limited to, Health Care Providers; Health Plans; individuals whose health information is contained within, or available through, a Participant’s System;; and employees, contractors, or agents of a Participant. A Participant User may act as either a Submitter, Recipient or both when Transacting Message Content.

hh. **Payment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

ii. **Performance and Service Specifications** shall mean the Validation Plan and the Specifications, as well as any implementation guidance, migration plans and other technical materials and resources approved by the Coordinating Committee in accordance with Section 10.03 of this Agreement.

jj. **Permitted Purpose** shall mean one of the following reasons for which Participants or Participant Users may legitimately Transact Message Content:

1. Treatment of the individual who is the subject of the Message;
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

2. Payment activities of the Health Care Provider for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan.

3. Health Care Operations of either
   .1. the Submitter if the Submitter is a Covered Entity;
   .2. a Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or
   .03. the Recipient if (i) the Recipient is a Health Care Provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such Health Care Provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such Health Care Provider;

4. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e);

5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. “Meaningful use of certified electronic health record technology” shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and

6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual’s personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.

kk. Protected Health Information or PHI shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.

ll. Receiving Party shall mean a Participant that receives Confidential Participant Information in any capacity including, but not limited to, as a member of the Coordinating Committee, from a Discloser.

mm. Recipient shall mean the Participant(s) or Participant User(s) that receives Message Content through a Message from a Submitter for a Permitted Purpose. For purposes of illustration only, Recipients include, but are not limited to, Participants or Participant Users who receive queries, responses, subscriptions, publications or unsolicited Messages.
nn. **Specifications** shall mean the specifications adopted by the Coordinating Committee pursuant to this Agreement to prescribe the data content, technical, and security requirements to enable the Participants to Transact Message Content. Specifications may include, but are not limited to, specific Network standards, services and policies. The Specifications are attached hereto as Attachment 1, and may be amended from time to time in accordance with Sections 10.02 and 10.03.

oo. **Submitter** shall mean the Participant(s) or Participant User(s) who submits Message Content through a Message to a Recipient for a Permitted Purpose. For purposes of illustration only, Submitters include, but are not limited to, Participants or Participant Users who push Messages with Message Content, send Messages seeking Message Content, send Messages in response to a request, send subscription Messages, or publish Messages with Message Content in response to subscription Messages.

pp. **System** shall mean software, portal, platform, or other electronic medium controlled by a Participant through which the Participant conducts its health information exchange related activities. For purposes of this definition, it shall not matter whether the Participant controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

qq. **Testing** shall mean the tests and demonstrations of a Participant’s System and processes used for interoperable health information exchange, to assess conformity with the Specifications and Validation Plan.

rr. **Transact** shall mean to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content using the Performance and Service Specifications.

ss. **Transaction Pattern** shall mean a type of information exchange service(s) enabled by the Specifications. The Operating Policies and Procedures will identify the Transaction Pattern(s) and the Specifications required to implement each Transaction Pattern. As of December 2010, the Transaction Patterns are submission, query and respond, publish and subscribe, and routing. The Transaction Patterns may be amended from time to time through amendment of the Specifications and the Operating Policies and Procedures.

tt. **Treatment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

uu. **Validation Plan** shall mean the framework for Testing and demonstrations for parties seeking to become Participants. The Validation Plan is attached hereto as Attachment 2, and as amended from time to time in accordance with Sections 10.02 and 10.03.

2. **Incorporation of Recitals.** The Recitals set forth above are hereby incorporated into this Agreement in their entirety and shall be given full force and effect as if set forth in the body of this Agreement.
3. **Purpose of the DURSA.**

3.01. The purpose of this Agreement is to provide a legal framework that will enable Participants to Transact Message Content with other Participants using the Performance and Service Specifications.

3.02. This Agreement hereby amends the November 18, 2009 Data Use and Reciprocal Support Agreement in its entirety, which has been entered into by some of the Participants.

4. **Coordinating Committee.**

4.01. **Formation of the Coordinating Committee.** To support the Participants who wish to Transact Message Content with other Participants, there shall be a Coordinating Committee.

4.02. **Composition of the Coordinating Committee.** The Coordinating Committee shall be composed of representatives of the Charter Participants and the Affiliation Groups as described more specifically herein. The Coordinating Committee is authorized to adopt, pursuant to the process in Section 11.03, Operating Policies and Procedures that modify the composition of the Coordinating Committee in response to a change in Federal law or regulation that results in a modification of the Participant eligibility requirements set forth in the Operating Policies and Procedures.

   a. **Charter Participant Representatives.** “Charter Participants” shall mean the first five Federal Participants and the first five Non-Federal Participants that actively engage in Transacting Message Content.

      Until September 30, 2014, each of the Charter Participants shall be entitled to appoint one individual to serve as that Charter Participant’s representative on the Coordinating Committee so long as the Charter Participant continues to be a Participant. Prior to September 30, 2013, the Coordinating Committee shall determine a process for evaluating continuation of the Charter Participants’ representation on the Coordinating Committee after September 30, 2014.

   b. **Affiliation Group Representatives.** “Affiliation Group” shall mean (i) all those Non-Federal Participants who are eligible to Transact Message Content in connection with a contract, grant, or cooperative agreement issued by the same Federal agency; or (ii) a Federal Participant and those Non-Federal Participants who are Transacting Message Content with it. By way of example only, all those Non-Federal Participants who are eligible to Transact Message Content in connection with a contract issued by ONC would be considered an “Affiliation Group.” By way of example only, the Social Security Administration (SSA)
and those Non-Federal Participants who are Transacting Message Content with SSA would be considered an “Affiliation Group.”

Annually, each Affiliation Group shall be entitled to select one individual to serve as the Affiliation Group’s representative on the Coordinating Committee. The initial term of an Affiliation Group representative shall commence upon that person’s selection by the Affiliation Group and end on September 30th of the following year. After this initial term, the selected representative of an Affiliation Group shall serve a one-year term from October 1 of one year until September 30th of the following year. The Coordinating Committee shall adopt Operating Policies and Procedures to define the manner in which the selection of a representative of an Affiliation Group is conducted.

The selected individual shall be either an employee or contractor of a Participant in that Affiliation Group. If the selected individual ceases to be an employee or contractor of a Participant in that Affiliation Group, the Affiliation Group shall be entitled to select a new representative on the Coordinating Committee to serve the remaining term of that individual.

The Coordinating Committee is authorized to adopt, pursuant to the process in Section 11.03, Operating Policies and Procedures to allow one or more Affiliation Groups to each select more than one representative if the number of Participants in the smallest Affiliation Group is less than 25% of the number of Participants in the largest Affiliation Group. In no case, however, may the Coordinating Committee adopt Operating Policies and Procedures that expand membership of the Coordinating Committee beyond twenty-one voting members.

c. **ONC Representative.** ONC shall be entitled to appoint an ex-officio, non-voting representative to serve on the Coordinating Committee.

d. In no case shall a Participant have more than one employee or contractor serving concurrently as representatives on the Coordinating Committee.

4.03. **Grant of Authority.** The Participants hereby grant to the Coordinating Committee the right to provide oversight, facilitation and support for the Participants who Transact Message Content with other Participants by conducting activities including, but not limited to, the following:

a. Determining whether to admit a New Participant;

b. Maintaining a definitive list of all Transaction Patterns supported by each of the Participants;

c. Developing and amending Operating Policies and Procedures in accordance with Section 11 of this Agreement;

d. Receiving reports of Breaches and acting upon such reports in accordance with Section 14.03 of this Agreement (Breach Notification);
e. Suspending or terminating Participants in accordance with Section 19 of this Agreement (Suspension and Termination);
f. Resolving Disputes between Participants in accordance with Section 21 of this Agreement (Dispute Resolution);
g. Managing the amendment of this Agreement in accordance with Section 23.02 of this Agreement;
h. Evaluating, prioritizing and adopting new Performance and Service Specifications, changes to existing Performance and Service Specifications and the artifacts required by the Validation Plan in accordance with Section 10 of this Agreement;
i. Maintaining a process for managing versions of the Performance and Service Specifications, including migration planning;
j. Evaluating requests for the introduction of Emergent Specifications into the production environment used by the Participants to Transact Message Content;
k. Coordinating with ONC to help ensure the interoperability of the Performance and Service Specifications with other health information exchange initiatives including, but not limited to, providing input into the broader ONC specifications activities and ONC Standards and Interoperability Framework initiatives; and
l. Fulfilling all other responsibilities delegated by the Participants to the Coordinating Committee as set forth in this Agreement.

To the extent permitted under Applicable Law, this grant of authority to the Coordinating Committee is unconditional and does not require any further consideration or action by any Participant.

The Coordinating Committee shall have the authority to unilaterally delegate to the Chairperson of the Coordinating Committee or a subcommittee of the Coordinating Committee any of the authorities, duties or responsibilities granted to the Coordinating Committee by the Participants. Any delegation of the Coordinating Committee’s authorities, duties or responsibilities to a designee other than the Chairperson of the Coordinating Committee or a subcommittee of the Coordinating Committee shall be accomplished through the adoption of Operating Policies and Procedures pursuant to Section 11.03.

4.04. In no case shall a Participant be required to disclose PHI to the Coordinating Committee in violation of Applicable Law. The Coordinating Committee shall not retaliate against a Participant that decides not to disclose PHI upon the request of the Coordinating Committee.

5. **Use of Message Content.**
5.01. **Permitted Purpose.** Participants shall only Transact Message Content for a Permitted Purpose as defined in this Agreement. Each Participant shall require that its Participant Users comply with this Section 5.01.

5.02. **Permitted Future Uses.** Subject to this Section 5.02 and Section 19.07, Recipients may retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient’s record retention policies and procedures. If the Recipient is a Participant that is a Business Associate of its Participant Users, such Participant may retain, use and re-disclose Message Content in accordance with Applicable Law and the agreements between the Participant and its Participant Users.

5.03. **Management Uses.** The Coordinating Committee may request information from Participants, and Participants shall provide requested information, for the purposes listed in Section 4.03 of this Agreement. Notwithstanding the preceding sentence, in no case shall a Participant be required to disclose PHI to the Coordinating Committee in violation of Applicable Law. Any information, other than Message Content, provided by a Participant to the Coordinating Committee shall be labeled as Confidential Participant Information and shall be treated as such in accordance with Section 16.

6. **System Access Policies.**

6.01. **Autonomy Principle.** Each Participant shall have Participant Access Policies. Each Participant acknowledges that Participant Access Policies will differ among them as a result of differing Applicable Law and business practices. Each Participant shall be responsible for determining whether and how to Transact Message Content based on the application of its Participant Access Policies to the information contained in the Message. The Participants agree that each Participant shall comply with the Applicable Law, this Agreement, and all applicable Performance and Service Specifications in Transacting Message Content.

6.02. **Identification.** Each Participant shall employ a process by which the Participant, or its designee, validates sufficient information to uniquely identify each person seeking to become a Participant User prior to issuing credentials that would grant the person access to the Participant’s System.

6.03. **Authentication.** Each Participant shall employ a process by which the Participant, or its designee, uses the credentials issued pursuant to Section 6.02 to verify the identity of each Participant User prior to enabling such Participant User to Transact Message Content.

7. **Enterprise Security.**

7.01. **General.** Each Participant shall be responsible for maintaining a secure environment that supports the operation and continued development of the Performance and Service Specifications. Participants shall use appropriate safeguards to prevent use or disclosure of Message Content other than as permitted by this Agreement, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Message Content. Appropriate
safeguards for Non-Federal Participants shall be those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, “required” implementation specifications, and “addressable” implementation specifications to the extent that the “addressable” implementation specifications are reasonable and appropriate in the Participant’s environment. If an “addressable” implementation specification is not reasonable and appropriate in the Participant’s environment, then the Participant must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate. Appropriate safeguards for Federal Participants shall be those required by Applicable Law related to information security. Each Participant shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the Participant’s respective Effective Date. Participants shall also be required to comply with any Performance and Service Specifications or Operating Policies and Procedures adopted by the Coordinating Committee, respectively, that define expectations for Participants with respect to enterprise security.

7.02. **Malicious Software.** Each Participant shall ensure that it employs security controls that meet applicable industry or Federal standards so that the information and Message Content being Transacted and any method of Transacting such information and Message Content will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, “malware,” or other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a System or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this Section.

8. **Equipment and Software.** Each Participant shall be responsible for procuring, and assuring that its Participant Users have or have access to, all equipment and software necessary for it to Transact Message Content. Each Participant shall ensure that all computers and electronic devices owned or leased by the Participant and its Participant Users to be used to Transact Message Content are properly configured, including, but not limited to, the base workstation operating system, web browser, and Internet connectivity.

9. **Auditing.** Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the Performance and Service Specifications.

10. **Performance and Service Specifications.**
10.01. **General Compliance.**

   a. **Transaction Patterns.** Each Participant shall implement and maintain at least one Transaction Pattern as a Submitter, a Recipient or both. Each Participant shall implement and maintain a Transaction Pattern only after appropriate approval and validation by the Coordinating Committee in accordance with the Operating Policies and Procedures.

   b. **Performance and Service Specifications.** Each Participant shall comply with (i) all of the Performance and Service Specifications applicable to the Transaction Pattern(s) that the Participant implements and maintains; and (ii) those Performance and Service Specifications identified by the Coordinating Committee as applicable to all Participants.

10.02. **Adoption of Performance and Service Specifications.** The Participants hereby grant the Coordinating Committee or its designee the right to adopt new Performance and Service Specifications, and to adopt amendments to, or repeal and replacement of, the Performance and Service Specifications at any time through the Performance and Service Specification Change Process described in Section 10.03.

10.03. **Performance and Service Specification Change Process.**

   a. **Participant Comment Period.** Prior to approving any new, amended, repealed or replaced Performance and Service Specification, the Coordinating Committee shall solicit and consider comments from the Participants on the new, amended, repealed or replaced Performance and Service Specification.

   b. **Objection Period.** Following the Coordinating Committee’s approval of the new, amended, repealed or replaced Performance and Service Specification, the Participants shall be given thirty (30) calendar days to review the approved Performance and Service Specification and register an objection if the Participant believes that the new, amended, repealed or replaced Performance and Service Specification will have a significant adverse operational or financial impact on the Participant. Such objection shall be submitted to the Coordinating Committee and contain a summary of the Participant’s reasons for the objection.

   c. **Approval of Changes to the Performance and Service Specifications.**

      1. **Less Than One-Third of Participants Object.** If the Coordinating Committee receives objections from less than one-third of the Participants during the thirty (30) calendar day objection period, the new, amended, repealed or replaced Performance and Service Specification shall go into effect as approved by the Coordinating Committee and on the date identified by the Coordinating Committee, unless the Coordinating Committee withdraws the new, amended, repealed or replaced Performance and Service Specification prior to such date. Consistent with Section 10.03(d), the effective date identified by the Coordinating
Committee may not be any earlier than the end of the thirty (30) calendar day objection period.

2. **More Than One-Third of Participants Object.** If the Coordinating Committee receives objections from one-third or more of the Participants during such thirty (30) day period, the Coordinating Committee shall review the new, amended, repealed or replaced Performance and Service Specification in light of the objections and make a determination as to how to modify the new, amended, repealed or replaced Performance and Service Specification, if at all. Once the Coordinating Committee finalizes its determination, it shall communicate this determination to the Participants and seek their approval. At least two-thirds of the Non-Governmental Participants and at least two-thirds of the Governmental Participants must approve the new, amended, repealed or replaced Performance and Service Specification for it to become effective.

d. **Implementation.** The Coordinating Committee shall provide Notice of new, amended, repealed or replaced Performance and Service Specification at least thirty (30) calendar days prior to the effective date of such new, amended, repealed or replaced Performance and Service Specification. This thirty (30) calendar day period may run concurrently with the thirty (30) calendar day objection period. Within fifteen (15) calendar days of receiving Notice of the new, amended, repealed or replaced Performance and Service Specification, a Participant may request that the Coordinating Committee delay implementation of such the new, amended, repealed or replaced Performance and Service Specification based on good cause. The Coordinating Committee shall respond to a request to delay implementation within seven (7) calendar days of receiving the request.

e. **Participant Duty to Terminate Participation.** If, as a result of a change made by the Coordinating Committee in accordance with this Section 10.03, a Participant will not be able to comply with the Performance and Service Specifications or does not otherwise desire to continue to Transact Message Content with other Participants after such change becomes effective, then such Participant shall terminate this Agreement accordance with Section 19.02.

11. **Operating Policies and Procedures.**

11.01. **General Compliance.** Each Participant shall comply with the Operating Policies and Procedures adopted by the Coordinating Committee in accordance with this Agreement.

11.02. **Development of the Operating Policies and Procedures.** The Participants hereby grant the Coordinating Committee the power to develop new Operating Policies and Procedures, and to amend, or repeal and replace, the Operating Policies and Procedures at any time through the Operating Policies and Procedures Change Process described in Section 11.03.

a. Participant Comment Period. Prior to approving any new, amended, repealed or replaced Operating Policies and Procedures, the Coordinating Committee shall solicit and consider comments from the Participants on the new, amended, repealed or replaced Operating Policies and Procedures.

b. Objection Period. Following the Coordinating Committee’s approval of the new, amended, repealed or replaced Operating Policies and Procedures, the Participants shall be given thirty (30) calendar days to review the approved Operating Policies and Procedures and register an objection if the Participant believes that the new, amended, repealed or replaced Operating Policies and Procedures will have a significant adverse operational or financial impact on the Participant. Such objection shall be submitted to the Coordinating Committee and contain a summary of the Participant’s reasons for the objection.

c. Approval of Changes to the Operating Policies and Procedures.

1. Less Than One-Third of Participants Object. If the Coordinating Committee receives objections from less than one-third of the Participants during the thirty (30) calendar day objection period, the new, amended, repealed or replaced Operating Policies and Procedures shall go into effect as approved by the Coordinating Committee and on the date identified by the Coordinating Committee, unless the Coordinating Committee withdraws the new, amended, repealed or replaced Operating Policies and Procedures prior to such date. Consistent with Section 11.03(d), the effective date identified by the Coordinating Committee may not be any earlier than the end of the thirty (30) day calendar objection period.

2. More Than One-Third of Participants Object. If the Coordinating Committee receives objections from one-third or more of the Participants during such thirty (30) calendar day period, the Coordinating Committee shall review the new, amended, repealed or replaced Operating Policies and Procedures in light of the objections and make a determination as to how to modify the new, amended, repealed or replaced Operating Policies and Procedures, if at all. Once the Coordinating Committee finalizes its determination, it shall communicate this determination to the Participants and seek their approval. At least two-thirds of the Non-Governmental Participants and at least two-thirds of the Governmental Participants must approve the new, amended, repealed or replaced Operating Policies and Procedures for them to become effective.

d. Implementation. The Coordinating Committee shall provide Notice of new, amended, repealed or replaced Operating Policies and Procedures at least thirty (30) calendar days prior to the effective date of such new, amended, repealed or replaced Operating Policies and Procedures. This thirty (30) calendar day period may run concurrently with the thirty (30) calendar day objection period.
Within fifteen (15) calendar days of receiving Notice of the new, amended, repealed or replaced Operating Policies and Procedures, a Participant may request that the Coordinating Committee delay implementation of such the new, amended, repealed or replaced Operating Policies and Procedures based on good cause. The Coordinating Committee shall respond to a request to delay implementation within seven (7) calendar days of receiving the request.

12. **Expectations of Participants.**

12.01. **Minimum Requirement for Participants that request Message Content for Treatment.**

   a. All Participants that request, or allow their respective Participant Users to request, Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A Participant shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. All responses to Messages shall comply with Performance and Service Specifications, this Agreement, any agreements between Participants and their Participant Users, and Applicable Law. Participants may, but are not required to, Transact Message Content for a Permitted Purpose other than Treatment. Nothing in this Section 12.01(a) shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.

   b. Each Participant that requests, or allows its respective Participant Users to request, Message Content for Treatment shall Transact Message Content with all other Participants for Treatment, in accordance with Sections 6, 12.01(a) and 14 of this Agreement. If a Participant desires to stop Transacting Message Content with another Participant based on the other Participant’s acts or omissions in connection with this Agreement, the Participant may temporarily stop Transacting Message Content with such Participant either through modification of its Participant Access Policies or through some other mechanism, to the extent necessary to address the Participant’s concerns. If any such cessation occurs, the Participant shall provide a Notification to the Coordinating Committee of such cessation and the reasons supporting the cessation. The Participants shall submit the Dispute leading to the cessation to the Dispute Resolution Process in Section 21. If the cessation is a result of a Breach that was reported to, and deemed resolved by, the Coordinating Committee pursuant to Section 14.03, the Participants involved in the Breach and the cessation shall engage in the Dispute Resolution Process in Section 21 in an effort to attempt to reestablish trust and resolve any security concerns arising from the Breach.

12.02. **Participant Users and HSPs.** Each Participant shall require that all of its Participant Users and HSPs Transact Message Content only in accordance with the terms and
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

conditions of this Agreement, including without limitation those governing the use, confidentiality, privacy, and security of Message Content. Each Participant shall discipline appropriately any of its employee Participant Users, or take appropriate contractual action with respect to contractor Participant Users or HSPs, who fail to act in accordance with the terms and conditions of this Agreement relating to the privacy and security of Message Content, in accordance with Participant’s employee disciplinary policies and procedures and its contractor and vendor policies and contracts, respectively.

12.03. License to Common Participant Resources. Participant is hereby granted a nonexclusive, nontransferable, revocable and limited license to Common Participant Resources solely for use as a Participant in performance of this Agreement. Participant shall not (a) sell, sublicense, transfer, exploit or, other than pursuant to this Agreement, use any Common Participant Resources for Participant's own financial benefit or any commercial purpose, or (b) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code to any Common Participant Resources. THE COMMON PARTICIPANT RESOURCES ARE PROVIDED “AS IS” AND “AS AVAILABLE” WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

13. Specific Duties of a Participant When Submitting a Message. Whenever a Participant or Participant User acts as a Submitter by submitting a Message to another Participant or Participant User, the Submitter shall be responsible for:

13.01. Submitting each Message in compliance with Applicable Law, this Agreement, the applicable Performance and Service Specifications, and Operating Policies and Procedures including, but not limited to, representing that the Message is:

(i) for a Permitted Purpose;
(ii) submitted by a Submitter who has the requisite authority to make such a submission;
(iii) supported by appropriate legal authority for Transacting the Message Content including, but not limited to, any consent or Authorization, if required by Applicable Law; and
(iv) submitted to the intended Recipient.

13.02. Representing that assertions or statements related to the submitted Message are true and accurate, if such assertions or statements are required by the Performance and Service Specifications or Operating Policies and Procedures;

13.03. Submitting a copy of the Authorization, if the Submitter is requesting Message Content from another Participant or Participant User based on the Permitted Purpose described in Section 1(jj)(6). Nothing in this Section shall be interpreted as requiring...
a. Each Participant agrees that within one (1) hour of discovering information that leads the Participant to reasonably believe that a Breach may have occurred, it shall alert other Participants whose Message Content may have been Breached.
and the Coordinating Committee to such information. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, the Participant shall provide a Notification to all Participants likely impacted by the Breach and the Coordinating Committee of such Breach. The Notification should include sufficient information for the Coordinating Committee to understand the nature of the Breach. For instance, such Notification could include, to the extent available at the time of the Notification, the following information:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content Breached
- Participants likely impacted by the Breach
- Number of individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by the Participant to mitigate the Breach
- Current Status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and the Coordinating Committee in accordance with Section 20(e) of this Agreement. The Notification required by this Section 14.03 shall not include any PHI. If, on the basis of the Notification, a Participant desires to stop Transacting Message Content with the Participant that reported a Breach, it shall stop Transacting Message Content in accordance with Section 12.01(b) of this Agreement. If, on the basis of the notification, the Coordinating Committee determines that (i) the other Participants that have not been notified of the Breach would benefit from a summary of the Notification or (ii) a summary of the Notification to the other Participants would enhance the security of the Performance and Service Specifications, it may provide, in a timely manner, a summary to such Participants that does not identify any of the Participants or individuals involved in the Breach.

b. Information provided by a Participant in accordance with this Section 14.03, except Message Content, may be “Confidential Participant Information.” Such “Confidential Participant Information” shall be treated in accordance with Section 16.

c. This Section 14.03 shall not be deemed to supersede a Participant’s obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law.

d. Compliance with this Section 14.03 shall not relieve Participants of any other security incident or breach reporting requirements under Applicable Law.
15. **Representations and Warranties.** Each Participant hereby represents and warrants the following:

15.01. **Accurate Participant Information.** Except to the extent prohibited by Applicable Law, each Participant has provided, and shall continue to provide, the Coordinating Committee with all information reasonably requested by the Coordinating Committee and needed by the Coordinating Committee to discharge its duties under this Agreement or Applicable Law, including during the Dispute Resolution Process. Any information provided by a Participant to the Coordinating Committee shall be responsive and accurate. Each Participant shall provide Notice to the Coordinating Committee if any information provided by the Participant to the Coordinating Committee materially changes. Each Participant acknowledges that the Coordinating Committee reserves the right to confirm or otherwise verify or check, in its sole discretion, the completeness and accuracy of any information provided by a Participant at any time and each Participant shall reasonably cooperate with the Coordinating Committee in such actions, given reasonable prior notice.

15.02. **Execution of the DURSA.** Prior to Transacting Message Content with other Participants, each Participant shall have executed this Agreement and returned an executed copy of this Agreement to the Coordinating Committee. In doing so, the Participant affirms that it has full power and authority to enter into and perform this Agreement and has taken whatever measures necessary to obtain all required approvals or consents in order for it to execute this Agreement. The representatives signing this Agreement on behalf of the Participants affirm that they have been properly authorized and empowered to enter into this Agreement on behalf of the Participant.

15.03. **Compliance with this Agreement.** Except to the extent prohibited by Applicable Law, each Participant shall comply fully with all provisions of this Agreement. To the extent that a Participant delegates its duties under this Agreement to a third party (by contract or otherwise) and such third party will have access to Message Content, that delegation shall be in writing and require the third party, prior to Transacting Message Content with any Participants, to agree to the same restrictions and conditions that apply through this Agreement to a Participant.

15.04. **Agreements with Participant Users.** Each Participant has valid and enforceable agreements with each of its Participant Users that require the Participant User to, at a minimum: (i) comply with all Applicable Law; (ii) reasonably cooperate with the Participant on issues related to this Agreement; (iii) Transact Message Content only for a Permitted Purpose; (iv) use Message Content received from another Participant or Participant User in accordance with the terms and conditions of this Agreement; (v) as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant; and (vi) refrain from disclosing to any other person.
any passwords or other security measures issued to the Participant User by the Participant. Notwithstanding the foregoing, for Participant Users who are employed by a Participant or who have agreements with the Participant which became effective prior to the Effective Date, compliance with this Section 15.04 may be satisfied through written policies and procedures that address items (i) through (vi) of this Section 15.04 so long as the Participant can document that there is a written requirement that the Participant User must comply with the policies and procedures.

15.05. **Agreements with Technology Partners.** To the extent that a Participant uses technology partners in connection with the Participant’s Transaction of Message Content, each Participant affirms that it has valid and enforceable agreements with each of its technology partners, including HSPs, that require the technology partner to, at a minimum: (i) comply with Applicable Law; (ii) protect the privacy and security of any Message Content to which it has access; (iii) as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant; and (iv) reasonably cooperate with the other Participants to this Agreement on issues related to this Agreement, under the direction of the Participant.

15.06. **Compliance with Specifications, Policies and Procedures.** Each Participant affirms that it fully complies with the Performance and Service Specifications and the Operating Policies and Procedures as more fully discussed in Sections 10.01 and 11.01 of this Agreement.

15.07. **Creation of Test Data.** Certain Participants agreed to anonymize PHI to create Test Data to be used by other Participants for Testing. Any Test Data that has been created, or will be created in the future, shall not contain PHI and has been, or will be, created in accordance with the Validation Plan.

15.08. **Accuracy of Message Content.** When acting as a Submitter, each Participant, in accordance with Section 17.02, hereby represents that at the time of transmission, the Message Content it provides is (a) an accurate representation of the data contained in, or available through, its System, (b) sent from a System that employs security controls that meet industry standards so that the information and Message Content being transmitted are intended to be free from malicious software in accordance with Section 7.02, and (c) provided in a timely manner and in accordance with the Performance and Service Specifications and Operating Policies and Procedures. Other than those representations in Sections 16.07, 16.08 and 16.09, the Submitter makes no other representation, express or implied, about the Message Content.

15.09. **Express Warranty of Authority to Transact Message Content.** To the extent each Participant is a Submitter and is providing Message Content to a Recipient, each Participant represents and warrants that it has sufficient authority to Transact such Message Content.

15.10. **Use of Message Content.** Each Participant hereby represents and warrants that it shall
use the Message Content only in accordance with the provisions of this Agreement.

15.11. **Compliance with Laws.** Each Participant shall, at all times, fully comply with all Applicable Law relating to this Agreement, the Transaction of Message Content for a Permitted Purpose and the use of Message Content.

15.12. **Absence of Final Orders.** Each Participant hereby represents and warrants that, as of the Effective Date, it is not subject to a final order issued by any Federal, State, local or international court of competent jurisdiction or regulatory or law enforcement organization, which will materially impact the Participant’s ability to fulfill its obligations under this Agreement. Each Participant shall inform the Coordinating Committee if at any point during the term of this Agreement it becomes subject to such an order.

15.13. **Federal Program Participation.** Each non-Federal Participant hereby represents and warrants that it is not excluded, debarred, or otherwise ineligible from participating in Federal contracts, subcontracts, grants, and nonprocurement transactions ("Federal Programs"). Each non-Federal Participant shall immediately provide written Notice to the Coordinating Committee if it is suspended, proposed for debarment or other exclusion, or otherwise disqualified or declared ineligible from participating in a Federal Program for any reason, or is a party to a legal proceeding that may result in any such action.

16. **Confidential Participant Information.**

16.01. Each Receiving Party shall hold all Confidential Participant Information in confidence and agrees that it shall not, during the term or after the termination of this Agreement, redisclose to any person or entity, nor use for its own business or benefit, any information obtained by it in connection with this Agreement, unless such use or redisclosure is permitted by the terms of this Agreement.

16.02. Confidential Participant Information may be redisclosed as required by operation of law, provided that the Receiving Party immediately notifies the Discloser of the existence, terms and circumstances surrounding such operation of law to allow the Discloser its rights to object to such disclosure. If after Discloser's objection, the Receiving Party is still required by operation of law to disclose Discloser’s Confidential Participant Information, it shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

17. **Disclaimers.**

17.01. **Reliance on a System.** Each Participant acknowledges and agrees that: (i) the Message Content provided by, or through, its System is drawn from numerous sources, and (ii) it can only confirm that, at the time Message Content is Transacted, the information and Message Content Transacted are an accurate representation of data contained in, or available through, its System. Nothing in this Agreement shall
be deemed to impose responsibility or liability on a Participant related to the clinical accuracy, content or completeness of any Message Content provided pursuant to this Agreement. The Participants acknowledge that other Participants’ Digital Credentials may be activated, suspended or revoked at any time or the Participant may suspend its participation; therefore, Participants may not rely upon the availability of a particular Participant’s Message Content.

17.02. Incomplete Medical Record. Each Participant acknowledges that Message Content Transacted by Participants may not include the individual’s full and complete medical record or history. Such Message Content will only include that data which is the subject of the Message and available for exchange among Participants.

17.03. Patient Care. Message Content obtained through a Message is not a substitute for any Participant or Participant User, if that person/entity is a Health Care Provider, obtaining whatever information he/she/it deems necessary, in his/her professional judgment, for the proper treatment of a patient. The Participant or Participant User, if he/she/it is a Health Care Provider, shall be responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for his/her/its respective patients and clients resulting from, or in any way related to, the use of the Network standards, services and policies agreed to by the Participants pursuant to this Agreement or the Message Content made available thereby. None of the Participants, by virtue of executing this Agreement, assume any role in the care of any patient.

17.04. Carrier lines. All Participants acknowledge that the Transaction of Message Content between Participants is to be provided over various facilities and communications lines, and information shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, “carrier lines”) owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Participants’ control. Provided a Participant uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this Agreement, the Performance and Service Specifications, and the Operating Policies and Procedures, the Participants assume no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted over those carrier lines, which are beyond the Participants’ control, or any delay, failure, interruption, interception, loss, transmission, or corruption of any Message Content or other information attributable to transmission over those carrier lines which are beyond the Participants’ control. Use of the carrier lines is solely at the Participants’ risk and is subject to all Applicable Law.

17.05. No Warranties. EXCEPT AS REPRESENTED IN SECTIONS 13.02 AND 15.08, MESSAGE CONTENT IS PROVIDED “AS IS” AND “AS AVAILABLE” WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND
NONINFRINGEMENT. IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL THE PARTICIPANT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF THE PARTICIPANT HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING. THE PARTICIPANT DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS TRANSMISSIONS AND LOSS OF SERVICE RESULTING FROM COMMUNICATION FAILURES BY TELECOMMUNICATION SERVICE PROVIDERS OR OTHER THIRD PARTIES.

17.06. **Performance of the Network Standards, Services and Policies.** The Participant makes no representation, express or implied, as to the performance of the Network standards, services and policies agreed to by the Participants pursuant to this Agreement. This disclaimer is not intended to diminish or limit in any way the other representations and warranties that the Participant is making in this Agreement. It is intended to recognize that the overall performance of the Network standards, services and policies agreed to by the Participants is beyond the power of any individual Participant to control.

18. **Liability.**

18.01. **Participant Liability.** As between Participants to this Agreement: Each Participant shall be responsible for its acts and omissions and not for the acts or omissions of any other Participant. In circumstances involving harm to other Participants caused by the acts or omissions of individuals who Transact Message Content or Confidential Participant Information through the Participant or by use of any password, identifier, or log-on received or obtained directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant Users, each Participant shall be responsible for such harm to the extent that the individual's access was caused by the Participant's breach of the Agreement or its negligent conduct for which there is a civil remedy under Applicable Law. Notwithstanding any provision in this Agreement to the contrary, Participant shall not be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law. This section shall not be construed as a hold harmless or indemnification provision.

18.02. **Effect of Agreement.** Except as provided in Section 17.05 (“No Warranties”) and Article 22 (“Dispute Resolution”), nothing in this Agreement shall be construed to restrict a Participant’s right to pursue all remedies available under law for damages or other relief arising from acts or omissions of other Participants related to this Agreement, or to limit any rights, immunities or defenses to which a Participant or Participant User may be entitled under Applicable Law.
18.03. **Coordinating Committee Liability.** Each Participant has agreed to comply with this Agreement. Accordingly, the Participants shall not hold the Coordinating Committee or any of their members liable for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on a Participant’s System resulting from any Participant’s actions or failures to act, except to the extent such action or failure to act was directed by the Coordinating Committee.

19. **Term, Suspension and Termination.**

19.01. **Term.** The initial term of this Agreement shall be for a period of one year commencing on the Effective Date. Upon the expiration of the initial term, this Agreement shall automatically renew for successive one-year terms unless terminated pursuant to this Section 19.

19.02. **Suspension or Termination by Participant.**

a. A Participant may voluntarily suspend its own right to Transact Message Content for a valid purpose, as determined by the Coordinating Committee, by informing the Coordinating Committee and other Participants of its voluntary suspension in accordance with the Operating Policies and Procedures. Once a Participant has properly informed the Coordinating Committee and other Participants of its voluntary suspension, neither the Participant, nor its Participant Users, shall Transact Message Content until the voluntary suspension has ended and the Participant has informed the Coordinating Committee and other Participants that the suspension has ended in accordance with the Operating Policies and Procedures. During the period of the voluntary suspension, the Participant’s inability to Transact Message Content and comply with those terms this Agreement that require Transaction of Message Content shall not be deemed a breach of this Agreement. Any voluntary suspension shall be for no longer than ten (10) consecutive calendar days or for more than forty (40) calendar days during any twelve (12) month period, unless a longer period is agreed to by the Coordinating Committee.

b. A Participant may terminate its own right to Transact Message Content by terminating this Agreement, with or without cause, by giving the Coordinating Committee at least five (5) business days prior written Notice. Once proper Notice is given, the Coordinating Committee shall be empowered to revoke the Participant’s Digital Credentials as of the date of termination specified in the Notice. Once the Coordinating Committee revokes the Participant’s Digital Credentials, the Coordinating Committee shall provide Notice of such revocation to the remaining Participants.

19.03. **Suspension by Coordinating Committee.** Upon the Coordinating Committee completing a preliminary investigation and determining that there is a substantial likelihood that a Participant’s acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant; a
Participant User; the integrity or operation of the Performance and Service Specifications; or an individual whose Message Content is Transacted using the Performance and Service Specifications; the Participants hereby grant to the Coordinating Committee the power to summarily suspend, to the extent necessary to address the threat posed by the Participant, a Participant’s Digital Credentials, pending the submission and approval of a corrective action plan, as provided in this Section. Upon suspension, the Coordinating Committee shall immediately suspend the Participant’s Digital Credentials and within twelve (12) hours of suspending a Participant’s right to Transact Message Content (i) provide Notice of such suspension to all Participants; and (ii) provide to the suspended Participant a written summary of the reasons for the suspension. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three (3) business days or, if such submission is not reasonably feasible within three (3) business days, then at the earliest practicable time. If the Participant submits a plan of correction, the Coordinating Committee shall, within five (5) business days, review and either accept or reject the plan of correction. If the plan of correction is accepted, the Coordinating Committee shall, upon completion of the plan of correction, reinstate the Participant’s Digital Credentials and provide Notice to all Participants of such reinstatement. If the plan of correction is rejected, the Participant’s suspension will continue, during which time the Coordinating Committee and the Participant shall work in good faith to develop a plan of correction that is acceptable to both the Participant and the Coordinating Committee. At any time after the Coordinating Committee rejects a Participant’s plan of correction, either the Participant or the Coordinating Committee may submit a Dispute to the Dispute Resolution Process described in Section 21. If the Coordinating Committee and the Participant cannot reach agreement on a plan of correction through the Dispute Resolution Process, the Coordinating Committee may terminate the Participant in accordance with Section 19.04.

19.04. **Termination by Coordinating Committee.** The Participants hereby grant to the Coordinating Committee the power to terminate a Participant’s right to Transact Message Content as follows:

a. After taking a suspension action in accordance with Section 19.03 when there is a substantial likelihood that the Participant’s acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant, a Participant User, integrity or operation of the Performance and Service Specifications, or an individual whose Message Content is Transacted using the Performance and Service Specifications; or

b. In the event a Participant is in material default of the performance of a duty or obligation imposed upon it by this Agreement and such default has not been substantially cured within thirty (30) calendar days following receipt by the defaulting Participant of written Notice thereof from the Coordinating Committee.

A Participant whose Digital Credentials are revoked by virtue of termination may appeal such revocation through the Dispute Resolution Process. However, during the pendency of any such appeal, the Participant’s Digital Credentials may continue to be
revoked at the discretion of the Coordinating Committee.

19.05. **Effect of Termination.** Upon any termination of this Agreement for any reason, the terminated party shall cease to be a Participant and thereupon and thereafter neither that party nor its Participant Users shall have any rights to Transact Message Content with other Participants (unless such Participant Users have an independent right to Transact Message Content through another Participant). The Coordinating Committee shall revoke a terminated Participant’s Digital Credentials, which will terminate Participant’s ability to Transact Message Content. Once the Coordinating Committee revokes the Participant’s Digital Credentials, the Coordinating Committee shall provide Notice of such revocation to the remaining Participants. In the event that any Participant(s) is terminated, this Agreement will remain in full force and effect with respect to all other Participants. Certain provisions of this Agreement survive termination, as more fully described in Section 23.05 (Survival Provisions).

19.06. **Confidential Participant Information.** All information used, provided, or created in accordance with this Section 19, except for Message Content, shall be labeled as “Confidential Participant Information” and shall be treated as such in accordance with Section 16.

19.07. **Disposition of Message Content on Termination.** At the time of termination, Recipient may, at its election, retain Message Content on Recipient’s System in accordance with the Recipient’s document and data retention policies and procedures, Applicable Law, and the terms and conditions of this Agreement, including Section 5.02.

20. **Cooperation.** Each Participant understands and acknowledges that numerous activities with respect to this Agreement shall likely involve another Participant’s employees, agents, and third party contractors, vendors, or consultants. To the extent not legally prohibited, each Participant shall: (a) cooperate fully with the Coordinating Committee, each other Participant, and any such third parties with respect to such activities as they relate to this Agreement; (b) provide such information to the Coordinating Committee, each other Participant, or such third parties as they may reasonably request for purposes of performing activities related to this Agreement; (c) devote such time as may reasonably be requested by the Coordinating Committee to review information, meet with, respond to, and advise the Coordinating Committee or other Participants with respect to activities as they relate to this Agreement; (d) provide such reasonable assistance as may be requested by the Coordinating Committee when performing activities as they relate to this Agreement; and (e) subject to a Participant’s right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any foreseeable dispute or litigation or protecting a Participant’s Confidential Participant Information, provide information and assistance to the Coordinating Committee or other Participants in the investigation of Breaches and Disputes. In no case shall a Participant be required to disclose PHI in violation of Applicable Law. In
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

seeking another Participant’s cooperation, each Participant shall make all reasonable efforts to accommodate the other Participant’s schedules and reasonable operational concerns. A Participant shall promptly report, in writing, to any other Participant and the Coordinating Committee, any problems or issues that arise in working with the other Participant’s employees, agents, or subcontractors that threaten to delay or otherwise adversely impact a Participant’s ability to fulfill its responsibilities under this Agreement. This writing shall set forth in detail and with clarity the problems that the Participant has identified.

21. **Dispute Resolution.**

21.01. **General.** The Participants acknowledge that it may be in their best interest to resolve Disputes through an alternative dispute resolution process rather than through civil litigation. The Participants have reached this conclusion based upon the fact that the legal and factual issues involved in this Agreement are unique, novel, and complex and limited case law exists which addresses the legal issues that could arise from this Agreement. Therefore, the Participants shall submit Disputes related to this Agreement to the non-binding Dispute Resolution Process attached hereto as Attachment 6 and incorporated herein. Except in accordance with Section 21.02(a), if a Participant refuses to participate in the Dispute Resolution Process, such refusal shall constitute a material breach of this Agreement and may be grounds for termination in accordance with Section 19.04(b).

21.02. **Immediate Injunctive Relief.**

a. Notwithstanding Section 21.01, a Participant may be relieved of its obligation to participate in the Dispute Resolution Process if such Participant (i) believes that another Participant’s acts or omissions create an immediate threat to the confidentiality, privacy or security of Message Content or will cause irreparable harm to another party (Participant, Participant User, the integrity or operation of the Performance and Service Specifications, or consumer) and (ii) pursues immediate injunctive relief against such other Participant in a court of competent jurisdiction. The Participant pursuing immediate injunctive relief must provide a Notification to the Coordinating Committee of such action within 24 hours of filing for the injunctive relief and of the result of the action within 24 hours of learning of same.

b. If the injunctive relief sought in Section 21.02(a) is not granted and the Participant seeking such relief chooses to pursue the Dispute, the Participants must then submit to the Dispute Resolution Process in accordance with Section 21.01.

21.03. **Activities during Dispute Resolution Process.** Pending resolution of any Dispute under this Agreement, the Participants agree to fulfill their responsibilities in accordance with this Agreement, unless the Participant voluntarily suspends its right to Transact Message Content in accordance with Section 19.02(a), is suspended in accordance with Section 19.03, or exercises its right to cease Transacting Message Content in accordance with Section 12.01(b).
21.04. **Implementation of Agreed Upon Resolution.** If, at any point during the Dispute Resolution Process, all of the Participants to the Dispute accept a proposed resolution of the Dispute, the Participants agree to implement the terms of the resolution in the agreed upon timeframe.

21.05. **Reservation of Rights.** If, following the Dispute Resolution Process, in the opinion of any involved Participant, the mandatory Dispute Resolution Process failed to adequately resolve the Dispute, the Participant(s) may pursue any remedies available to it in a court of competent jurisdiction.

22. **Notices.** All Notices to be made under this Agreement shall be given in writing to the appropriate Participant’s representative at the address listed in Attachment 4 or the Coordinating Committee, and shall be deemed given: (i) upon delivery, if personally delivered; (ii) upon the date indicated on the return receipt, when sent by the United States Postal Service Certified Mail, return receipt requested; and (iii) if by facsimile telecommunication or other form of electronic transmission, upon receipt when the Notice is directed to a facsimile telecommunication number or electronic mail address listed on Attachment 4 and the sending facsimile machine or electronic mail address receives confirmation of receipt by the receiving facsimile machine or electronic mail address.

23. **Miscellaneous/General.**

23.01. **Governing Law.** In the event of a Dispute between or among the Participants arising out of this Agreement, the applicable Federal and State conflicts of law provisions that govern the operations of the Participants involved in the Dispute shall determine governing law.

23.02. **Amendment.** This Agreement may be amended by agreement of at least two-thirds of the Non-Governmental Participants and at least two-thirds of the Governmental Participants. However, if the change is required for the Coordinating Committee or Participants to comply with Applicable Law, the Coordinating Committee may implement the change with approval of at least a majority of Non-Governmental Participants and at least a majority of Governmental Participants and within a time period the Coordinating Committee determines is appropriate under the circumstances. All Participants shall be required to sign an amendment adopted in accordance with the provisions of this Section or terminate participation in accordance with Section 19.02.

23.03. **New Participants.** Upon the Coordinating Committee’s acceptance of a New Participant, the Coordinating Committee shall have the New Participant execute a Joinder Agreement, the form of which is attached hereto as Attachment 7. The Participants agree that upon execution of the Joinder Agreement by a duly authorized representative of the Coordinating Committee, all then-current Participants shall be deemed to be signatories to the Joinder Agreement with the result being that current Participants and the New Participant are all bound by this Agreement. The New Participant shall not be granted the right to Transact Message Content until both it and the Coordinating Committee execute the Joinder Agreement.
23.04. **Assignment.** No Party shall assign or transfer this Agreement, or any part thereof, without the express written consent of the Coordinating Committee. Any assignment that does not comply with the requirements of this Section 23.04 shall be void and have no binding effect.

23.05. **Survival.** The provisions of Sections 1, 5.02, 5.03, 14, 15.10, 16, 18, 19.06, 19.07, 20 and 21 shall survive the termination of this Agreement for any reason.

23.06. **Waiver.** No failure or delay by any Participant in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any right shall constitute a waiver of any prior, concurrent, or subsequent right.

23.07. **Entire Agreement.** This Agreement, together with all Attachments, sets forth the entire and only Agreement among the Participants relative to the subject matter hereof. Any representation, promise, or condition, whether oral or written, not incorporated herein, shall not be binding upon any Participant.

23.08. **Validity of Provisions.** In the event that a court of competent jurisdiction shall hold any Section, or any part or portion of any Section of this Agreement, invalid, void or otherwise unenforceable, each and every remaining Section or part or portion thereof shall remain in full force and effect.

23.09. **Priority.** In the event of any conflict or inconsistency between a provision in the body of this Agreement and any attachment hereto, the terms contained in the body of this Agreement shall prevail.

23.10. **Headings.** The headings throughout this Agreement are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify, or aid in the interpretation or construction of meaning of the provisions of this Agreement. All references in this instrument to designated “Sections” and other subdivisions are to the designated Sections and other subdivisions of this Agreement. The words “herein,” “hereof,” “hereunder,” and other words of similar import refer to this Agreement as a whole and not to any particular Section or other subdivision.

23.11. **Relationship of the Participants.** The Participants are independent contracting entities. Nothing in this Agreement shall be construed to create a partnership, agency relationship, or joint venture among the Parties. Neither the Coordinating Committee nor any Participant shall have any authority to bind or make commitments on behalf of another Participant for any purpose, nor shall any such Party hold itself out as having such authority. No Participant shall be held liable for the acts or omissions of another Participant.

23.12. **Counterparts.** With respect to the first two Participants to this Agreement, the Effective Date shall be the date on which the second Participant executes this Agreement. For all Participants thereafter, the Effective Date shall be the date that the Participant executes this Agreement or the Joinder Agreement, in accordance with
Section 23.03. This Agreement or the Joinder Agreement may be executed in any number of counterparts, each of which shall be deemed an original as against the Participant whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.

23.13. **Third-Party Beneficiaries.** With the exception of the Participants to this Agreement, there shall exist no right of any person to claim a beneficial interest in this Agreement or any rights occurring by virtue of this Agreement.

23.14. **Force Majeure.** A Participant shall not be deemed in violation of any provision of this Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other disruptive natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) terrorist attacks; (g) acts of legislative, judicial, executive, or administrative authorities; or (h) any other circumstances that are not within its reasonable control. This Section 23.14 shall not apply to obligations imposed under Applicable Law.

23.15. **Time Periods.** Any of the time periods specified in this Agreement may be changed pursuant to the mutual written consent of the Coordinating Committee and the affected Participant(s).

This Agreement has been entered into and executed by officials duly authorized to bind their respective parties.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Attachment 1 - Specifications

Accessible at: http://healthit.hhs.gov/nhinexchange
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Attachment 2 - Validation Plan and Test Materials

Accessible at: http://healthit.hhs.gov/nhinexchange
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Attachment 3 - Operating Policies and Procedures

Accessible at: http://healthit.hhs.gov/nhinexchange
Attachment 4 - Participant Addresses for Notice

<table>
<thead>
<tr>
<th>Name</th>
<th>Primary Contact</th>
<th>Alternate Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>City, State Zip</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pursuant to Section 14.01(d), the following HIPAA provisions are applicable to each Participant that is neither a Covered Entity, a Business Associate nor a Governmental Participant as if they were acting in the capacity of a Covered Entity. Definitions contained in the various provisions of 45 C.F.R. Parts 160 through 164 apply to the provisions listed in this Attachment 1 to the extent they are used in said sections.

- 45 C.F.R. § 164.306 (Security Rule – General rules)
- 45 C.F.R. § 164.308 (Security Rule – Administrative Safeguards)
- 45 C.F.R. § 164.310 (Security Rule – Physical Safeguards)
- 45 C.F.R. § 164.312 (Security Rule – Technical Safeguards)
- 45 C.F.R. § 164.314 (Security Rule – Organizational requirements)
- 45 C.F.R. § 164.316 (Security Rule – Policies and procedures and documentation requirements)
- 45 C.F.R. § 164.502, other than paragraphs (h), and (i) (Privacy Rule – Uses and disclosures of PHI: general rules) [see notes below for descriptions of excluded subsections]
- 45 C.F.R. § 164.504 (Privacy Rule – Uses and disclosures: Organizational requirements)
- 45 C.F.R. § 164.506 (Privacy Rule – Uses and disclosures to carry out treatment, payment, or health care operations)
- 45 C.F.R. § 164.508 (Privacy Rule – Uses and disclosures for which an authorization is required)
- 45 C.F.R. § 164.510 (Privacy Rule – Uses and disclosures requiring an opportunity to agree or to object)
- 45 C.F.R. § 164.512 (Privacy Rule – Uses and disclosures for which an authorization or opportunity to agree or object is not required)
- 45 C.F.R. § 164.514 (Privacy Rule – Other requirements relating to uses and disclosures of PHI)
- 45 C.F.R. § 164.520 (Privacy Rule – Notice of privacy practices for PHI)
- 45 C.F.R. § 164.522 (Privacy Rule – Rights to request privacy protection for PHI)
- 45 C.F.R. § 164.524 (Privacy Rule – Access of individuals to PHI)
- 45 C.F.R. § 164.528 (Privacy Rule – Accounting of disclosures of PHI)
- The following provisions of 45 C.F.R. § 160.530, but only to the extent that they relate to the above provisions. For example, with respect to 45 C.F.R. § 164.530(b), the Participant must
provide training with respect to the above provisions, such as § 164.506, but not with respect to other provisions of the HIPAA Regulations, such as § 164.522.

- 45 C.F.R. § 164.530(b) (Privacy Rule – Administrative Requirements, Training)
- 45 C.F.R. § 164.530(c) (Privacy Rule – Administrative Requirements, Safeguards)
- 45 C.F.R. § 164.530(d) (Privacy Rule – Administrative Requirements, Complaints to the Covered Entity)
- 45 C.F.R. § 164.530(e) (Privacy Rule – Administrative Requirements, Sanctions)
- 45 C.F.R. § 164.530(f) (Privacy Rule – Administrative Requirements, Mitigation)
- 45 C.F.R. § 164.530(g) (Privacy Rule – Administrative Requirements, Refraining from intimidating or retaliatory acts)
- 45 C.F.R. § 164.530(h) (Privacy Rule – Administrative Requirements, Waiver of rights)
- 45 C.F.R. § 164.530(i) (Privacy Rule – Administrative Requirements, Policies and procedures)
- 45 C.F.R. § 164.530(j) (Privacy Rule – Administrative Requirements, Documentation)

Notes:

The following requirements have not been included:

- 45 C.F.R. § 164.302 (Security Rule – Applicability)
- 45 C.F.R. § 164.304 (Security Rule – Definitions)
- 45 C.F.R. § 164.500 (Privacy Rule – Applicability)
- 45 C.F.R. § 164.501 (Privacy Rule – Definitions)
- 45 C.F.R. § 164.502(h) (Confidential communications), and (i) (Uses and disclosures consistent with notice)
- 45 C.F.R. § 164.526 (Privacy Rule – Amendment of PHI)
- 45 C.F.R. § 164.530(a) (Privacy Rule – Administrative Requirements, Personnel designations)
- 45 C.F.R. § 164.530(k) (Privacy Rule – Administrative Requirements, Group health plans)
- 45 C.F.R. § 164.532 (Privacy Rule – Transition provisions)
Attachment 6 - Dispute Resolution Process

When a Dispute arises, a Participant shall send written Notice, in accordance with the Notice provision in the DURSA, to the other Participant(s) involved in the Dispute. The notice must contain a summary of the issue as well as a recommendation for resolution. The Participant must send a copy of the notice to the Dispute Resolution Subcommittee (see below) for informational purposes.

Within thirty (30) calendar days of receiving the notice, the Participants are obligated to meet and confer with each other, at least once in good faith and at a mutually agreeable location (or by telephone), to try to reach resolution (the “Informal Conference”). If the Participants reach a resolution at the Informal Conference, they shall provide Notification to that effect to the Dispute Resolution Committee.

If the Participants are unable to participate in an Informal Conference during the thirty (30) calendar day period or to reach resolution at the Informal Conference, they have ten (10) business days following the end of the thirty (30) calendar day period or the Informal Conference, respectively, in which to escalate the Dispute to the Dispute Resolution Subcommittee in writing.

The Dispute Resolution Subcommittee (the “Subcommittee”) will be a five (5) member standing subcommittee of the Coordinating Committee. The Coordinating Committee shall appoint each member of the Subcommittee for a definite term. The members must be representative of the Participants, have diverse skill sets, and be able to help facilitate and reach resolution on conflicts between the Participants. The Subcommittee must have access to legal counsel to advise it on the law relevant to matters before it.

In addition to appointing the five (5) members of the Subcommittee, the Coordinating Committee must also appoint three (3) to five (5) alternates for the Subcommittee. Alternates will serve on the Subcommittee should any of the members have a conflict on a particular Dispute or in the event that a member(s) is unavailable. Subcommittee members are required to declare any conflicts in accordance with the Coordinating Committee’s conflict of interest policy. Once a Subcommittee member declares a conflict, the remaining Subcommittee members shall decide amongst themselves whether such member must withdraw from the Subcommittee for the dispute in question.

The Subcommittee must also have access to panels of subject matter experts, as identified by the Coordinating Committee, for a variety of topics that may be implicated by a Dispute. Each subject matter expert panel must have at least three (3) experts on it who will rotate as advisors to the Subcommittee.

Once a Participant escalates a Dispute to the Subcommittee, the Subcommittee will have thirty (30) calendar days in which to convene a meeting of the involved Participants (“Committee Meeting”). During this meeting, each Participant shall be able to present its
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

version of the Dispute and any information that it believes is pertinent to the Subcommittee’s decision.

- The Subcommittee shall have the ability to request additional information from the Participants to help it make its determination. The Subcommittee, however, shall not have the authority to compel a response or the production of testimony or documents by the Participants. To the extent that the Participants do respond to requests of the Subcommittee by producing documents, Participants shall have the ability to mark the documents produced as “Confidential Participant Information” and the Subcommittee shall treat those documents in accordance with Section 16 of the DURSA.

- The Subcommittee is encouraged to develop an appropriate and equitable resolution of each submitted Dispute, considering all available evidence, the goals of the Agreement and other relevant considerations. The Subcommittee must also have the authority to recommend sanctions for the breaching Participant. These sanctions include developing corrective action plans, suspension of participation rights, and termination of participation rights. The type of sanction will depend on the nature and severity of the breach.

- Within fifteen (15) calendar days of the Subcommittee Meeting, the Subcommittee shall issue a written recommendation for resolution, including an explanation of the basis and rationale of its recommendation. If either Participant is dissatisfied with the Subcommittee’s recommendation for resolution, it shall have five (5) business days in which to escalate the Dispute to the Coordinating Committee.

- Within twenty (20) calendar days of receiving notice of escalation from a Participant, the Coordinating Committee shall review the Subcommittee’s recommendation along with the information on which such recommendation was based and issue a final resolution. The Coordinating Committee may seek additional information from the Participants to aid its resolution of the Dispute.

- Within seven (7) calendar days of receiving the final resolution from the Coordinating Committee, the Participants shall determine whether to accept or reject the resolution and so notify the Coordinating Committee.

- The Coordinating Committee shall send a written summary of the resolution of the Dispute to all Participants. The summary will not identify the Participants involved, but will contain sufficient detail about the resolution to serve as an instructive resource for other Participants.

- In no case shall a Participant be required to disclose PHI in violation of Applicable Law as part of its participation in the Dispute Resolution Process. The decision to not disclose PHI shall not be held against a Participant in the Dispute Resolution Process.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Attachment 7 – Joinder Agreement

THIS JOINDER AGREEMENT made as of the last date set forth below, by and between the Coordinating Committee on behalf of the Participants (“Coordinating Committee”) and ___________________________ (the “New Participant”) makes New Participant a party to that certain Data Use and Reciprocal Support Agreement dated May 3, 2011 among the Participants, as amended through the date hereof (the “DURSA”).

RECITALS:

A. The New Participant desires to become a Participant and Transact Message Content with other Participants.

B. The Coordinating Committee has accepted and approved the New Participant’s application to become a Participant and Transact Message Content with other Participants, with the condition precedent that the New Participant executes this Joinder Agreement.

AGREEMENT:

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the undersigned hereby agree as follows:

1. JOINDER. The New Participant is hereby made a party to the DURSA, and agrees to be bound by, and shall comply with, the terms thereof. From the date hereof, the New Participant shall be a “Participant” as that term is defined in the DURSA and shall be subject to all of the duties and obligations and entitled to the rights and benefits of a “Participant” as provided therein.

2. ACKNOWLEDGEMENT. The New Participant hereby acknowledges that it has received and reviewed a copy of the DURSA.

4. REAFFIRMATION. The terms and provisions of the DURSA remain in full force and effect in all respects.

5. COUNTERPARTS. This Joinder Agreement may be executed in any number of counterparts, each of which shall be an original, but all of which taken together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the undersigned have caused this Joinder Agreement to be executed, all as of the day and year first written above.
Data Use and Reciprocal Support Agreement (DURSA)

Policy Assumptions

May 3, 2011

The DURSA is a comprehensive legal agreement used to establish trust for information exchanged among Participants in the eHealth Exchange. This agreement is based upon a set of policy assumptions that bridge varying state and federal laws and regulations, as well as differing local policies. The agreement, while articulated as a contract, underscores a framework for broad-based information exchange among a set of trusted entities who either wish to query and retrieve data or push data to others in the network.

The following outlines the key policy assumptions which underscore the agreement:

- **Shared Rules of the Road and Shared Governance.** Common framework that binds all Participants to a set of technical requirements, testing requirements, policies, governance structure and accountability measures, including a process for adding or changing requirements.

- **Representative Governance:** Participants are governed by a representative group of Participants who share data in production. Additional methods for obtaining broad community input and engagement (e.g. task groups, outreach, industry collaboration, etc.) shall be supported to assure support and alignment with national policy.

- **Participants in Production.** Assumes that participants are in production and leverages a participant’s existing end user trust agreements, policies and vendor agreements.

- **Multiple Exchange Methods and Profiles.** Enables Participants to declare which profiles or use cases they wish to support in production. Supports multiple exchange methods, or “Transaction Patterns”, such as: push, query / retrieve and publish/subscribe.

- **Privacy and Security Obligations.** Defers to Applicable Law and establishes HIPAA as contractual standard of performance for those who are not governmental agencies and not otherwise subject to HIPAA. Highlights specific requirements which represent the most likely risk to the network, related to: system access policies, identification, authentication, enterprise security, malicious software, auditing and monitoring access.

- **Identification and Authentication.** Each user who shares data as part of the eHealth Exchange shall be uniquely identified and their identity verified prior to granting access to a Participant’s system.

- **Permitted Purposes.** Permits exchange of information among eHealth Exchange Participants for certain purposes, including: treatment, limited payment and health care operations, public health activities and reporting, any purpose to demonstrate meaningful use, and disclosures based upon an individual’s authorization. These purposes may be revisited over time as additional use cases are brought forward.

- **Future Use of Data Received Through the eHealth Exchange.** Data are received and integrated into end-user’s system and may be reused or disclosed as any other information in its records, in accordance with Applicable Law and local record retention policies.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

- **Local autonomy** - Each Participant shall have Participant Access Policies that establish a Participant’s Users are permitted to exchange data using the Participant’s system. Each Participant acknowledges that these access policies will differ among them as a result of varying Applicable Law and business practices. A Participant may not discriminate and refuse to share data with another Participant solely on the basis of differing system access privileges. A Participant is not required or permitted to release information in conflict with Applicable Law.

- **Reciprocal Duty to Respond.** Participants who query data for treatment purposes also have a duty to respond to requests for data for treatment purposes, either with a copy of the data or with a standardized response that data are not available. Participants may respond to requests for other purposes.

- **Responsibilities of Party Submitting Data.** Participants who submit data are responsible for submitting the information in compliance with applicable law and representing that the message is:
  - for a Permitted Purpose;
  - sent by the Participant who has requisite authority to do so;
  - supported by appropriate legal authority, such as consent or authorization, if required by Applicable Law; and
  - sent to the intended recipient.

- **Authorizations.** When a request is based on an authorization (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data.

- **Participant Breach Notification.** Participants are required to promptly notify the eHealth Exchange Coordinating Committee and other impacted Participants of breaches related to the eHealth Exchange (i.e. unauthorized acquisition, access, disclosure or use of the data transmitted among participants, which occur while transmitting the data).

- **Chain of Trust.** A participant’s obligations to comply with the DURSA must “flow down” to users or other participating organizations that connect through a Participant’s system, as well as the technology partner.

- **Mandatory Non-Binding Dispute Resolution.** Participants will agree to participate in a mandatory, non-binding dispute resolution process that preserves the Participants’ rights to seek redress in the courts if not resolved through the dispute resolution process.

- **Allocation of Liability Risk.** Each participant is responsible for their own acts and omissions, but not the acts and omissions of other participants. Participants are responsible for harm caused if they breach the DURSA or if, due to their negligence, there is a breach of data being transmitted.

**Representations and Warranties:**

- Protected Health Information (PHI) may not be used in test data sets used for testing purposes. PHI may not be sent to the Coordinating Committee.

- Participants represent that the data they transmit is an accurate representation of the data in their system at the time the data are transmitted.
Participants warrant that they have the authority to transmit information.

Participants assert that they are not subject to a final order issued by a court, regulatory or law enforcement organization which materially impacts their ability to fulfill their obligations under the DURSA. In addition, participants represent that they are not excluded, debarred or ineligible for participating in federal contracts, or grants.

Participants do not guarantee clinical accuracy, content or completeness of the messages transmitted. Data transmitted do not include a full and complete medical record or history. In addition, data transmitted are not a substitute for health care providers to obtain whatever information they deem necessary to properly treat patients. Healthcare providers are accountable for treating patients. Participants, by virtue of signing the DURSA, do not assume any role in the care of an individual.

Participants are not accountable for failure of carrier lines (e.g. third party carriers for communications, Internet backbone, etc.) which are beyond the Participant’s control. Data are provided “as is” and “as available”, without a warranty of its “fitness for a particular purpose”.

Participants are not liable for erroneous transmissions, and loss of service resulting from communication failures by telecommunication service providers or other third parties.
Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into this ___ day of ________, _____ between [name of Covered Entity], a [state name][professional corporation] [partnership] [sole proprietorship] ("Physician Practice") and [name of Business Associate], a [type of business entity] ("Contractor").

RECITALS

Physician Practice is a [type of organization] that provides medical services with a principal place of business at [address].

Contractor is a [type of organization] that [description of primary functions or activities] with a principal place of business at [address].

Physician Practice, as a Covered Entity under the Health Information Portability and Accountability Act of 1996 ("HIPAA") is required to enter into this Agreement to obtain satisfactory assurances that Contractor, a Business Associate under HIPAA, will appropriately safeguard all Protected Health Information ("PHI") as defined herein, disclosed, created, maintained or received by Contractor on behalf of Physician Practice.

Physician Practice desires to engage Contractor to perform certain functions for, or on behalf of, Physician Practice involving the disclosure of PHI by Physician Practice to Contractor, or the
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

creation, maintenance or use of PHI by Contractor on behalf of Physician Practice, and Contractor desires to perform such functions.

This contract shall be deemed an amendment to the parties' underlying contract dated __________ ("Underlying Agreement").

In consideration of the mutual promises below and the exchange of information pursuant to this agreement and in order to comply with all legal requirements for the protection of this information, the parties therefore agree as follows:

Article I. Definitions of Terms

1.01 “Agreement” means this Business Associate Agreement.

1.02 “Business Associate” shall have the meaning given to such term in 45 C.F.R. § 160.103.

1.03 “C.F.R.” shall mean the Code of Federal Regulations.

1.04 “Covered Entity” shall have the meaning given to such term in 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

1.05 “Designated Record Set” shall have the meaning given to such term in 45 C.F.R. § 164.501.

1.06 “Electronic Protected Health Information or Electronic PHI” shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that Business Associate creates, receives, maintains or transmits from or on behalf of Physician Practice.

1.07 “HIPAA Rules” shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160
and 164.

1.08 “Individual” shall have the same meaning given to such term in 45 C.F.R. § 160.103 and shall include a person who qualifies as the individual’s personal representative in accordance with 45 C.F.R. § 164.502(g).

1.09 “Privacy Rule” shall mean the Privacy Standards at 45 C.F.R. Part 164, Subpart E.

1.10 “Protected Health Information” ("PHI") shall have the meaning given to such term in 45 C.F.R. § 160.103.

1.11 “Required By Law” shall have the same meaning given to such term in 45 C.F.R. § 164.103.

1.12 “Secretary” shall mean the Secretary of Health and Human Services (“HHS”) or his or her designee as provided in 45 C.F.R. § 160.103.

1.13 “Security Incident” shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 164.304.


Article II. Obligations and Activities of Contractor

2.01 Protected Health Information. Contractor agrees and acknowledges that any individual’s Protected Health Information that comes within Contractor’s custody, exposure, possession or knowledge or is created, maintained, retained, transmitted, derived, developed, compiled, prepared or used by Contractor in the course of or in connection with the performance of services under this Agreement, is confidential and shall remain the exclusive property of Physician Practice and shall be used, disclosed, transmitted and/or maintained solely in accordance with this Agreement and as
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Required By Law. Contractor agrees to comply with its obligations as a Business Associate and acknowledges that it is subject to and agrees to comply with HIPAA and all applicable guidance and regulations issued by the Secretary to implement HIPAA and all other applicable law.

2.02 Use of Protected Health Information. Contractor shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

2.03 Forwarding Requests for Disclosure from Government to Physician Practice. Contractor shall forward all requests for the disclosure of Protected Health Information from a law enforcement or government official, or pursuant to a subpoena, other legal request or court or administrative order, to Physician Practice as soon as possible before making the requested disclosure, but no later than five (5) business days following its receipt of such request or order.

2.04 Assisting Physician Practice Respond to Requests for Disclosure from Government. Contractor shall provide to Physician Practice all Protected Health Information necessary to respond to a request for the disclosure of Protected Health Information by a law enforcement or government official, or pursuant to a subpoena, other legal request, or court or administrative order as soon as possible, but no later than two (2) business days following its receipt of such written request from Physician Practice.

2.05 Restrictions on Use and/or Disclosure of Protected Health Information. Contractor shall comply with all granted restrictions on the use and/or disclosure of Protected Health Information, pursuant to 45 C.F.R. § 164.522(a), upon notice from Physician Practice. Contractor shall forward to Physician Practice any requests for restriction on the use and/or disclosure of Protected
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Health Information within five (5) business days of receipt.

2.06 Requests for Confidential Communication of Protected Health Information. Contractor shall comply with all granted requests for confidential communication of Protected Health Information, pursuant to 45 C.F.R. § 164.522(b), upon notice from Physician Practice. Contractor shall forward to Physician Practice any requests for confidential communication of Protected Health Information within ten (10) business days of receipt.

2.07 Appropriate Safeguards. Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Physician Practice, as required by the Security Rule.

2.08 Duty to Mitigate. Contractor shall take immediate steps to mitigate, to the extent practicable or as reasonably directed by Physician Practice, any harmful effect that is known to Contractor of a use or disclosure of Protected Health Information by Contractor in violation of the requirements of this Agreement, the Privacy Rule or the Security Rule, such as obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.

2.09 Reporting of Unauthorized Uses or Disclosures. Contractor shall report to Physician Practice any use or disclosure of the Protected Health Information not provided for by this Agreement, the Privacy Rule or the Security Rule, including breaches of unsecured Protected Health Information, as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware, as soon as possible, but no later than five (5) business days after discovery, stating (to the extent known by Contractor) the nature of such use or disclosure, the names and addresses of the individuals
who are the subject of such Protected Health Information and the names of the individuals who made or engaged in such use or disclosure and any other available information that the Physician Practice is required to include in notifications to the affected individuals.

2.10 Subcontractors, Consultants, Agents and Other Third Parties. Contractor shall in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2) ensure that any subcontractor, consultant, agent, or other third party that creates, receives, maintains, or transmits Protected Health Information on behalf of Contractor agrees to the same restrictions, conditions, and requirements that apply to Contractor with regard to its creation, use, and disclosure of Protected Health Information. Contractor shall, upon request from Physician Practice, provide Physician Practice with a list of all such third parties. Contractor shall ensure that any subcontractor, consultant, agent, or other third party to whom it provides Electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect such information. Contractor must terminate its agreement with any subcontractor, consultant, agent or other third party, and obtain all Protected Health Information provided to such subcontractor, consultant, agent or other third party, if Contractor becomes aware that the subcontractor, consultant, agent or other third party has breached its contractual duties relating to HIPAA or this agreement. If any subcontractor, consultant, agent, or other third party of Contractor are not subject to the jurisdiction or laws of the United States, or if any use or disclosure of Protected Health Information in performing services under the Agreement will be outside of the jurisdiction of the United States, such entities must agree by written contract with the Contractor to be subject to the jurisdiction of the Secretary, the laws and the courts of the United States, and waive any available jurisdictional defenses as they pertain to the parties’ obligations under this Agreement, the
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Privacy Rule or the Security Rule.

2.11 Books and Records. Contractor shall make internal practices, books, and records relating to Protected Health Information received from, or created or received by Contractor, on behalf of Physician Practice, available to Physician Practice, or at the request of Physician Practice to the Secretary, for purposes of the Secretary determining Physician Practice’s compliance with the Privacy Rule.

2.12 Documenting Disclosures. Contractor shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for Physician Practice 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.

2.13 Accounting for Disclosures. Contractor shall provide to Physician Practice, upon request and in the time and manner required by 45 C.F.R. § 164.528(c)(1), an accounting of disclosures of an Individual’s Protected Health Information, collected in accordance with Section 2.11 of this Agreement, to permit Physician Practice 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.

2.14 Minimum Necessary. Contractor acknowledges that it shall request from the Physician Practice and so disclose to its affiliates, subsidiaries, agents, subcontractors or other third parties, only the minimum Protected Health Information necessary to perform or fulfill a specific function required or permitted hereunder. Contractor acknowledges that the Secretary is required by the Health Information Technology for Economic and Clinical Health “HITECH Act” to issue guidance on what constitutes “minimum necessary” for purposes of the Privacy Standards. Contractor agrees to comply with the guidance, once issued by the Secretary.
and to only request, use or disclose the minimum amount of Protected Health Information as described in such guidance.

2.15 **Training.** Contractor shall provide training as to the Privacy Rule and the Physician Practice’s privacy policy to all of its employees who will handle or be responsible for handling Protected Health Information on the Physician Practice’s behalf.

2.16 **Independent Contractor.** The relationship of the Contractor with Physician Practice shall be one of independent contractor, and not an employee or agent of Physician Practice.

2.17 **Securing Protected Health Information.** Contractor will comply with Section II.B of the April 27, 2009 HHS guidance (74 Fed. Reg. 19006 at 19009-19010) setting forth the technologies and methodologies for rendering Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. Contractor shall insure that any subcontractor, consultant, agent, vendor, or other third party to whom it provides Protected Health Information will implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act and HHS guidance specifies with respect to rendering Physician Practice’s Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

2.18 **Breach Notification.** Notwithstanding paragraph 2.17 above, if any Protected Health Information in the possession, custody or control of Contractor remains or becomes unsecured, Contractor shall, following discovery of a breach (as such term is defined in 45 C.F.R. § 164.402) of such unsecured Protected Health Information, provide the notifications to individuals, the media and the Secretary, as set forth in 45 C.F.R. §§ 164.404 through 164.408.

2.19 **Timeliness of Notifications.** Except where a law enforcement
official states to Physician Practice or Contractor that a notification would impede a criminal investigation or cause damage to national security, all notifications shall be made without unreasonable delay and in no case later than 60 calendar days from discovery of the breach.

2.20 **Indemnification.** Contractor shall defend, indemnify and hold harmless the Physician Practice from and against any or all cost (including but not limited to any and all costs incurred by Covered Entity in complying with the breach notification requirements of 45 C.F.R. Part 164, Subpart D), loss, interest, damage, liability, claim, legal action or demand by third parties, (including costs, expenses and reasonable attorney fees on account thereof) arising out of Contractor’s activities under the Agreement, including but not limited to, any breach of unsecured Protected Health Information by the Contractor or failure by the Contractor to provide the breach notifications required by 45 C.F.R. §§ 164.404 through 164.408, except to the extent that such loss, interest, damage, liability, claim, legal action or demand was incurred as a result of the negligence or willful misconduct of Physician Practice. As a condition precedent to the Contractor’s obligation to indemnify Physician Practice under this Agreement, Physician Practice must notify Contractor within a reasonable amount of time upon learning of any claim or liability in order to give Contractor an opportunity to present any appropriate defense on behalf of Physician Practice and Contractor. Physician Practice shall have the right, but not the obligation, to participate in any defense at its own cost and with its own counsel. The provisions of this paragraph 2.20 will survive the termination of this Agreement.

2.21 **Application of Privacy Rule to Contractor.** Where provided, the standards, requirements, and implementation specifications adopted under 45 C.F.R. Part 164, Subpart E, apply to Contractor with respect to the Protected Health Information of Physician Practice.
2.22 Fundraising. Contractor agrees to clearly and conspicuously provide any recipient of fundraising communications the opportunity to opt out of receiving any further such solicitations.

2.23 Sale of Protected Health Information. Contractor shall, except pursuant to and in compliance with 45 C.F.R. § 164.508(a)(4), not engage in the sale of Protected Health Information.

2.24 Compliance and Enforcement. Contractor is subject to the compliance, enforcement and civil monetary penalties provisions at 45 C.F.R., Part 160, Subparts C and D.

2.25 Individual’s Access to Protected Health Information. Contractor shall cooperate with Physician Practice on a timely basis, consistent with 45 C.F.R. § 164.524(b)(2), to fulfill all requests by individuals for access to the individual’s Protected Health Information that are approved by Physician Practice. Contractor shall make available Protected Health Information in a designated record set to Physician Practice as necessary to satisfy Physician Practice’s obligations under 45 C.F.R. § 164.524(c). Contractor further agrees that to the extent Contractor maintains Protected Health Information of Physician Practice in an electronic health record (“EHR”), Physician Practice must comply with patients’ requests for access to their Protected Health Information by giving them, or any entity that they designate clearly, conspicuously and specifically, the information in an electronic format, and must not charge the requestor more than the labor costs in responding to the request for the copy (or summary or explanation).

2.26 Implement Information Security Program. Contractor shall implement a documented information security program that includes administrative, technical and physical safeguards designed to prevent the accidental or otherwise unauthorized use or disclosure of Protected Health Information, and the integrity and
availability of electronic Protected Health Information it creates, receives, maintains or transmits on behalf of Physician Practice. The security program shall include reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. In addition, Contractor agrees to (1) maintain written documentation of its policies and procedures, and any action, activity or assessment which the HIPAA Security Rule requires to be documented, (2) retain this documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later, (3) make this documentation available to those persons responsible for implementing the procedures to which the documentation pertains, and (4) review this documentation periodically, and update it as needed in response to environmental or operational changes affecting the security of the electronic Protected Health Information. Contractor agrees to encrypt all electronic Protected Health Information and destroy all paper Protected Health Information such that it is unusable, unreadable, or indecipherable to unauthorized users. Upon request, Contractor shall make available Contractor’s security program, including the most recent electronic Protected Health Information risk analysis, policies, procedures, security incidents and responses and evidence of training.

2.27 Amendments to Protected Health Information. Contractor shall make any amendment(s) to Protected Health Information in a designated record set as directed or agreed to by Physician Practice pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Physician Practice’s obligations under 45 C.F.R. § 164.526. Contractor must act on an individual’s request for an amendment in a manner and within the time period set forth in 45 C.F.R. § 164.526(b)(2).

2.28 Marketing. Contractor shall not use or disclose Protected Health Information for marketing purposes without the
individual’s authorization, except as provided in 45 C.F.R. §§ 164.508(a)(3)(i)(A) and (B).

Article III. Permitted Uses and Disclosures by Contractor

3.01 General Use and Disclosure. Except as otherwise limited in this Agreement, Contractor may use or disclose Protected Health Information only to perform its obligations and services to Physician Practice or as Required By Law, provided that such use or disclosure would not violate the Privacy or Security Rule if done by Physician Practice.

3.02 Specific Use and Disclosure Provisions.

3.02.01 Management and Administration of Contractor. Except as otherwise limited in this Agreement, Contractor may use Protected Health Information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

3.02.02 Other Uses and Disclosures. Except as otherwise limited in this Agreement, and notwithstanding Section 3.01 above, Contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that disclosures are Required by Law, or Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will be held 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 Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

3.02.03 Data Aggregation Services. Contractor may use Protected Health Information to provide data aggregation services to Physician Practice as permitted by 42 C.F.R. §
3.02.04 Reporting Violations of the Law. Contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.51(f).

3.02.05 Reporting to Health Plan. Contractor will not disclose Protected Health Information to a health plan if the individual to whom the Protected Health Information pertains has so requested and (1) the disclosure would be for the purposes of payment or health care operations, and not for the purposes of treatment, (2) the Protected Health Information at issue pertains to a health care item or service for which the individual pays out-of-pocket and in full and (3) the disclosure is not required by law.

3.02.06 Minimum Necessary. Contractor will, in the performance of its obligations and services to Physician Practice make reasonable efforts to use, disclose and request only the minimum amount of Physician Practice’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except as set forth in 45 C.F.R. § 164.502(b)(2).

Article IV. Obligations of Physician Practice

4.01 Provisions for Physician Practice to Inform Contractor of Privacy Practices and Restrictions.

4.01.01 Upon Contractor’s request, Physician Practice shall provide Contractor with the notice of privacy practices that Physician Practice produces in accordance with 45 C.F.R. § 164.520, as well as any changes to that notice.

4.01.02 Physician Practice shall provide Contractor with
any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information, if such changes affect Contractor’s permitted or required uses and disclosures.

4.01.03 Physician Practice shall notify Contractor, in writing, of any restriction to the use or disclosure of Protected Health Information that Physician Practice has agreed to in accordance with 45 C.F.R. § 164.522, and Contractor agrees to conform to any such restriction.

4.01.04 Physician Practice acknowledges that it shall provide to, or request from, the Contractor only the minimum Protected Health Information necessary for Contractor to perform or fulfill a specific function required or permitted hereunder.

4.01.05 Physician Practice shall take immediate steps to mitigate an impermissible use or disclosure of Protected Health Information from Contractor to Physician Practice, including its staff, employees and agents who send and receive Protected Health Information to and from Contractor in the course and scope of their employment, such as obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means between Physician Practice and its staff, employees and agents) or will be destroyed.

4.02 Permissible Requests by Physician Practice

Physician Practice represents and warrants that it has the right and authority to disclose Protected Health Information to Contractor for Contractor to perform its obligations and provide services to Physician Practice. Physician Practice shall not request Contractor to use or disclose Protected Health Information in any
manner that would not be permissible under the Privacy Rule if done by Physician Practice.

Article V. Term and Termination

5.01 **Term.** The provisions of this Agreement shall take effect ____________. Except as otherwise provided herein, the Agreement shall terminate when all of the Protected Health Information provided by Physician Practice to Contractor, or created or received by Contractor on behalf of Physician Practice, is destroyed or returned to Physician Practice.

5.02 **Termination for Cause.** Upon a Party’s knowledge of a material breach by the other party, the non-breaching Party shall provide an opportunity for the breaching Party to cure the breach or end the violation and terminate this Agreement if the breaching Party does not cure the breach or end the violation within the time specified by the non-breaching Party or immediately terminate this Agreement if cure of such breach is not possible.

5.03 **Termination Without Cause.** Either party to this Agreement may terminate the Agreement upon provision of [sixty (60)] days prior written notice.

[NOTE: Ensure the notice period is long enough to allow for replacement of the services.]

5.04 **Effect of Termination.**

5.04.01 **Disposal of PHI.** Except as provided in paragraph 5.04.02 of this Section, upon termination of this Agreement, for any reason, Contractor shall return or destroy all Protected Health Information received from Physician Practice, or created or received by Contractor on behalf of Physician Practice, at the direction of Physician Practice. Contractor shall request, in writing, Protected Health Information that is in the possession of subcontractors or
agents of Contractor.

5.04.02 In the event the Contractor determines that returning or destroying the Protected Health Information is infeasible, Contractor shall provide to Physician Practice notification of the conditions that make return or destruction infeasible. If return or destruction of Protected Health Information is infeasible, Contractor shall extend the protection of this Agreement to such Protected Health Information, for so long as Contractor maintains such Protected Health Information. Following the termination of this Agreement, Contractor shall not disclose Protected Health Information except to Physician Practice or as Required by Law.

Article VI. Miscellaneous

6.01 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

6.02 Amendment. This Agreement may be amended upon the mutual written agreement of the parties. Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, and by mutual agreement, amend the Agreement in such manner as such party determines necessary to comply with such law, policy, decision or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Agreement on thirty (30)
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

days written notice to the other party.

6.03 **Survival.** The obligations of Contractor under Section 5.04.02 of this Agreement shall survive the termination of this Agreement.

6.04 **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Physician Practice to comply with the HIPAA Rules. In the event of any inconsistency or conflict between this Agreement and any other agreement between the parties, the terms, provisions and conditions of this Agreement shall govern and control. In the event of an inconsistency between the provisions of the Agreement and the mandatory terms of the HIPAA Rules, as may be amended from time to time by HHS or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the Parties, the interpretation of HHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence. Where provisions of this Agreement are different from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of the Agreement shall control.

6.05 **No third party beneficiary.** Nothing express or implied in this Agreement is intended to confer, and nothing herein shall confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.

6.06 **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois. Any disputes relating to this Agreement shall be resolved by the state or federal courts located in Chicago, Illinois, and Contractor consents to venue in those courts as proper.
IN WITNESS WHEREOF, the parties hereto have duly executed this agreement to be effective as of [effective date of the agreement].

Physician Practice

By: ______________________
Name: _____________________
Title: ______________________
Date: ______________________

Contractor

By: ______________________
Name: _____________________
Title: ______________________
Date: ______________________
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Opt-Out or Opt-Back-In Form
for the Pennsylvania Health Information Exchange Network

Please initial that you have read and understand each of the following statements.

By submitting this Opt-Out Form my medical information will NOT be accessible to health care providers and other authorized users, (including for emergency services) through the Pennsylvania Health Information Exchange Network (P3N, Pa Patient and Provider Network).

Initial

Initial here only if submitting this form as an Opt-Back-In request.

Initial

This request does not preclude my health care provider from otherwise disclosing my medical information pursuant to other authorizations and applicable laws, or by other methods, including fax.

Initial

I may choose to participate in the PA Health Information Exchange Network again at any time by submitting this form as an Opt-Back-In form.

Initial

First Name: ____________________________ Middle Name: ____________________________ Last Name: ____________________________

Maiden Name: ____________________________ Date of Birth: ____________________________ (Ex: 12/15/1991)

Gender: Female Male

Street Address: ________________________________________________________________

City: ____________________________ State: ________________ Zip Code: ________________

Phone 1: ____________________________ Phone 2 ____________________________ (optional): ____________________________

Last Four (4) Digits of Social Security Number(optional): ____________________________ (Ex. xxx-xx-1234)

Email Address(optional): ________________________________________________________

Patient Signature: X Date Signed: ____________________________

(Signature of parent, legal guardian, or legal representative, where required)

Print Name: ____________________________ Relationship to the Patient: ____________________________

This form must be returned with original signatures in black or blue ink. All non-optional fields must be filled out in order for your request to be processed. A separate form must be filled out for each family member. A contact phone number is required in case we must contact you to ensure the accuracy of your demographic information. You will receive an acknowledgement of the receipt of this form.

Return Form To:
Pennsylvania eHealth Partnership Authority
402A Finance Building
Harrisburg, Pennsylvania 17120
ra-paehealth@pa.gov
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

The Pennsylvania eHealth Initiative in collaboration with the Pennsylvania eHealth Partnership Authority
May 14, 2014

Ensuring Privacy and Security of Health information Exchange in Pennsylvania

Steven J. Fox, Esq.
Principal, Post & Schell, P.C.

William “Buddy” Gillespie
Director Healthcare Solutions, DSS
Introduction

The Pennsylvania eHealth Initiative (PAeHI) is a not-for-profit founded in 2005 by the state’s leading healthcare organizations to transform healthcare by fostering the broader adoption of electronic health records and health information exchange.

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.

Purpose

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.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 5

**Background**

In 2009, PAeHI published a white paper entitled “Ensuring Privacy and Security of Health Information Exchange in Pennsylvania”:

This paper was well received and given the distinguished honor of being published in the Spring 2009 HIMSS Journal of Health Information Management (JHIM).

However, since then a lot of changes, coupled with significant progress, have taken place across the healthcare spectrum. To name a few, a growing number of HIEs have achieved sustainability, Meaningful Use Stage I has taken place, and the Final Ruling (Omnibus Bill) for HIPAA was introduced into law.

This poster available in pdf format on PAeHI website.
Patients are unlikely to share sensitive health information unless they are confident that their provider will honor their confidentiality. Similarly, health care entities are unlikely to join a health information exchange if they are not confident that their medical records will be kept safe and that the data will be flowing securely.

A key factor in achieving a high level of trust and compliance among individuals, health care providers, and other health care organizations participating in a health information exchange is the development of, and adherence to, a consistent and coordinated approach to privacy and security. Clear, understandable and uniform principles are a first step in developing this approach to privacy and security while building trust, which are all essential to the realization of the considerable benefits of HIE.
Executive Summary

• It can be a challenge to adopt clear and uniform privacy and security principles in a legal landscape that seems inconsistent and restrictive. Absorbing those principles into a sustainable business model that hits all its required regulatory marks requires strong leadership and the will to get it done to both support the business goals and serve the patients and consumers of Pennsylvania.

Executive Summary

• In 2012, the Commonwealth established the Pennsylvania eHealth Partnership Authority as the governance entity for HIE in the state. The Authority is moving forward with all the mandates contained in its founding legislation to provide uniform standards and agreements that are produced in concert with stakeholders, along with freely distributed consumer outreach tools and a state consent registry.
Executive Summary

- PAeHI sees this as the first vital step in Pennsylvania achieving a truly interoperable health information exchange network that both supports and expands the market for such services.
- The broad topic discussions and outlines contained in this white paper are presented as a tool to spur further thinking about the appropriate methods to interface with the legal requirements as to electronic health information privacy and security, the specific requirements within Pennsylvania, and the workplace challenges of technical and administrative implementation.

Key Definitions

- Privacy
  - (1) The right to have all records and information pertaining to health care treated as confidential.
  - (2) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue, unauthorized, or illegal gathering and use of data about that individual. (HIMSS, 2006)
Key Definitions

• 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.

Key Definitions

• Omnibus Final Rules
– The Omnibus final rule clarifications were released in January 2013 to provide additional rulemaking around the HIPAA Privacy and Security Rules. The Omnibus rule was based on statutory changes under the HITECH Act and the Genetic Information Nondiscrimination Act of 2008 (GINA).
Key Definitions

- PA eHealth Information Technology Act
  - This Act, also known as Act 121 of 2012, established the Pennsylvania eHealth Partnership Authority (Authority) as an independent agency of the Commonwealth and the governance body for the statewide technological health information exchange network it was to build.

Landscape and Roadmap

- The health care industry has had many spirited discussions regarding privacy and security from both the provider and patient perspectives since HIPAA was enacted in 1996. The issues surrounding privacy and security continue to challenge all stakeholders regardless of technological sophistication, particularly those involved in the direct delivery of care. This tension between privacy and security requires collaborative solutions that fairly balance the competing interests between security implemented from a business perspective and with an eye to the bottom line, and the privacy rights and expectations of individuals as to their medical information.
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 17

Landscape and Roadmap

What is Currently Required?
- Policies & Procedures
  - Legal
  - Regulatory
  - Organizational
  - Personal

What is Currently Required?
- Policies & Procedures
  - Legal
  - Regulatory
  - Organizational
  - Personal

Slide 18

Slide 125
What is Currently Required?

• Policies & Procedures
  – Trust Agreements Among Care Providers
  – Consumer Consent/Authorization
  – Business Associate Agreements
  – Data Use & Reciprocal Support Agreements (DURSA)
  – Risk Management & Framework
  – Identification of Threats
  – Mitigation Strategies
  – Communication with Stakeholders

What is Currently Required?

• Conforming to Policies & Controlling Risks
  – Administrative Controls
  – Procedural Controls
  – Physical and environmental Controls
  – Technical Controls
  – Handling Residual Risk
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 21

What is Currently Required?

• Workforce Considerations
  – Security is about people
  – Appropriate & repeated training is key to successful health information sharing
  – Most breaches due to employee mistakes & negligence, not hacking or bad intent
  – BYOD contributes to increasing risk
  – More privacy risk assessments would reduce frequency of unintentional data breaches

Slide 22

What are Enabling Solutions?

• Best Practices
• Stakeholder Education
• Key Technical Properties
• Demonstration & Model Projects
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 23

What are New Compliance Challenges?

- Checkbox Compliance
- PHI Ownership & Disposal
- Proprietary EHRs/HIEs
- Convergence of HIOs & Social Media
- BI and Data Analytics

Slide 24

What are New Compliance Challenges?

- Checkbox Compliance
- PHI Ownership & Disposal
- Proprietary EHRs/HIEs
- Convergence of HIOs & Social Media
- BI and Data Analytics
What are Emerging Areas of Risk?

- Cloud Hosting
- Cyber Security Insurance
- Cyber Attacks
- Mobile Device Management & BYOD
- Physician & Patient Portals
- Backup and Disaster Recovery

Key Documents

- Data Use and Reciprocal Support Agreement (DURSA)
- Business Associate Agreements (BAA)
- PA Opt-Out Form
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 27

Timeline

• Nov, 2013 (Review Objectives)
• Jan, 2014 (Draft Revised Report)
• March, 2014 (Webinar review with stakeholders)
• April, 2014
  • DVHIMSS Presentation
  • KINBER Presentation
  • CHOP Poster Presentation
  • Final Report
• May 14, 2014 Presentation at 10th Annual PAeHI Summit

Contributors

PA eHealth Initiative
• Robert Torres, Esq.
• Steven J. Fox, Esq.
• William “Buddy” Gillespie
• Dr. Chris Cavanaugh
• And special thanks to the PAeHI Committees (BHOX and Policy)

PA eHealth Partnership Authority
• Alix Goss
• R. Roberts

Slide 28
Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Slide 29

For further information: www.paehi.org
Steven J. Fox
Chair, Policy Committee
sjfox@postschell.com

Buddy Gillespie
Chair, Business, Health Outcomes and HIE Committee
wgillespie@dsscorp.com

Slide 30

Thank You!
Discussion

Page 131
PAeHI wishes to thank William “Buddy” Gillespie of DSS, Steve Fox Esq. from Post & Schell, P.C., and Chris Cavanaugh for their invaluable help in preparing this updated white paper. PAeHI also wishes to acknowledge the contributions of Alix Goss, Executive Director of the Pennsylvania eHealth Partnership Authority, and R. Roberts, Research Coordinator at the Authority, for their contributions.

PAeHI BOARD OF DIRECTORS
2013 - 2014

Board of Directors

Robert Torres, Esq. (Chair), Capital Blue Cross
Kenneth D. Coburn, MD (Vice Chair), Health Quality Partners
Martin J. Ciccocioppo (Secretary), HAP
Bernie Lynch (Treasurer), Pennsylvania Medical Society
Sharon L. Dorogy (Past Chair), The Children's Institute
Edith Dees, Holy Spirit Hospital
Steve Fox, Esq., Post & Schell, PC
William "Buddy" Gillespie, DSS
Alix Goss, PA eHealth Partnership Authority
Phil Magistro, Quality Insights of Pennsylvania
Jean Stretton, MD, Gateway Medical Association
Charles Stuckey, OD, Pennsylvania Optometric Association

Ex Officio Board Members

Leslie Amoros, Amoros Communications, C&E Committee Vice-Chair
Thompson Boyd, III, MD, CPHIMS, Hahnemann University Hospital, BHOX Vice-Chair
Gus Geraci, MD, Pennsylvania Medical Society, C&E Committee Chair
Augusta "Gus" Kairys, Highmark, BHOX Committee Vice-Chair
Don Levick, MD, Lehigh Valley Health Network, Finance Committee Vice-Chair
Susan M. Salkowitz, MA MGA, Salkowitz Associates, LLC, BHOX Committee Vice-Chair
Senator Randy Vulakovich, Chairman of the Communications and Technology Committee

Staff

Executive Director, Chris Cavanaugh, EdD, PAeHI