Pennsylvania's Journey for
Health Information Exchange

CERT Symposium: Cyber Security
Incident Management for Health Information Exchanges

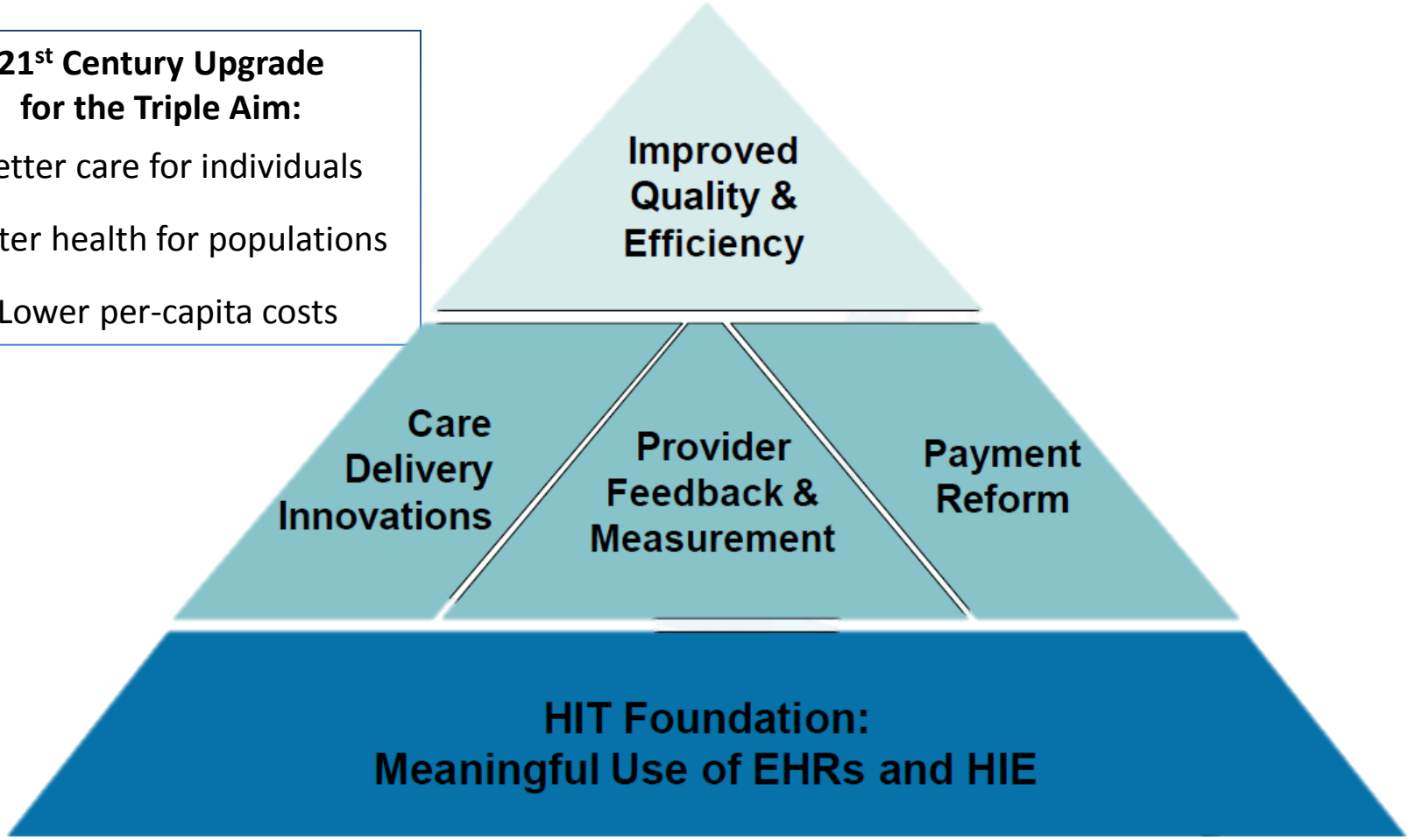
June 26, 2013
Pittsburgh, PA

PA eHEALTH PARTNERSHIP AUTHORITY

The Journey to the Triple AIM

21st Century Upgrade for the Triple Aim:

- Better care for individuals
- Better health for populations
- Lower per-capita costs



Slide adapted from Trudi Matthews, HealthBridge/Greater Cincinnati Beacon Collaboration Presentation at ONC Meeting 4/3/13

PA eHEALTH PARTNERSHIP AUTHORITY

Makeover for Healthcare

- Uncoordinated care
- Over-loaded schedule
- Physician & practice-centric
- Arbitrary quality improvement projects
- Lack of clear leadership & support (for patient centered primary care)

- Team-based approach
- Open access
- Patient engagement & empanelment
- Data directed quality improvement efforts
- Engaged leadership

Slide adapted from Trudi Matthews, HealthBridge/Greater Cincinnati Beacon Collaboration Presentation at ONC Meeting 4/3/13

PA's Transformation Journey

Collaborative "system" to achieve consensus and produce outcomes

- Diverse stakeholder engagement in open and transparent manner
- Data driven decision-making
- Iterative and layered approach to design and problem solving
  - ~ Blended diverse views create better steps forward
  - ~ Incrementally address issues

Pennsylvania HIE Strategic Plan

Stakeholders Recommended:

- Establish public/private authority to become overarching HIE governing entity after federal grant ends and then transition to independent non-profit organization
- Authority will provide “community shared services” to enable and advance health information exchange within and beyond PA among disparate organizations
- Federated model - all participants maintain their own information and no health data will be centrally stored
- One-to-many connection to achieve related efficiencies for public and private sector health information exchanges
- Multiple exchange ‘tools’

PA eHEALTH PARTNERSHIP AUTHORITY

Stakeholder Collaboration

Participant Workgroup engaged to:

- Recommend approach for *technical* infrastructure and services
- Identify *policy and operational* framework and training considerations related to privacy and security
- Solidify *sustainability* model
- Establish criteria for *certification* program

Federal Government

HealtheWay (Formerly NwHIN)
Interstate Exchange

Other States and Territories

Provider Directory

Enterprise Master Patient Index

PA eHealth Partnership Authority's Governance and Community Shared Services

Opt-Out Registry

Record Locator Service

Internet Connectivity and Access

PA Certified HIEs, including the Commonwealth Internal-HIE and Other Like Entities

PA Certified HISPs & Like Entities

Pharmacies

Labs

Clinics/ Hospitals

Long-term Care Facilities

Patients

Providers

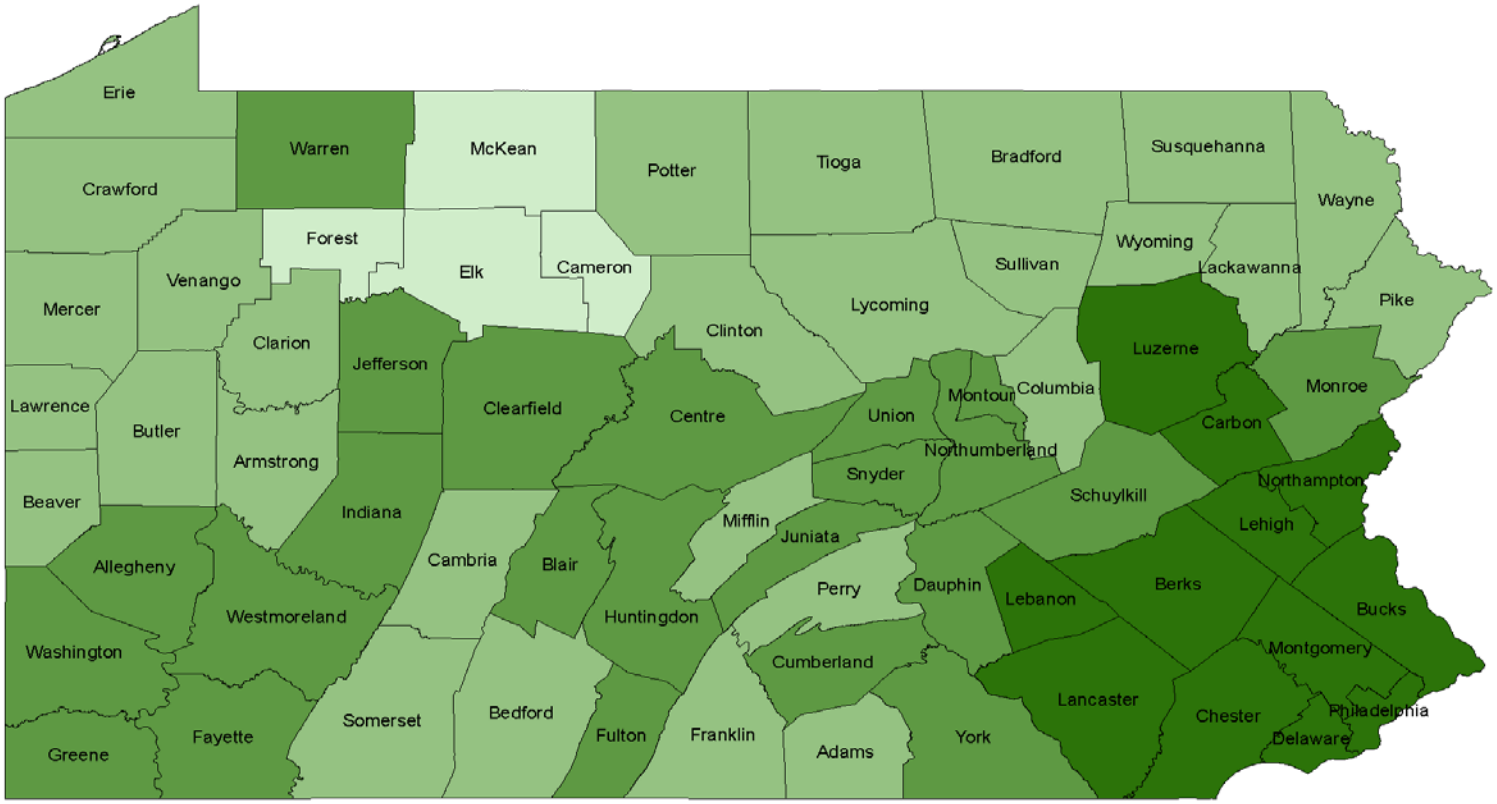
Continuation of Care Team

Payers/ Health Plans

Other Individuals & Teams

Planned HIE Coverage

Pennsylvania HIEs



HIEs by County

1 2 3 4 5 - 7

Note: All PA counties are served by at least two (2) health information exchanges (HIE).

Legal, Privacy and Security

PA eHEALTH PARTNERSHIP AUTHORITY

Legal, Privacy and Security

The Nationwide Privacy and Security Framework

8 Principles (ONC, 2008)

1) **INDIVIDUAL ACCESS.** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format

2) **CORRECTION.** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied

Legal, Privacy and Security

The 8 Principles (ONC, 2008), continued

3) **OPENNESS AND TRANSPARENCY.** There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information

4) **INDIVIDUAL CHOICE.** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information

Legal, Privacy and Security

The 8 Principles (ONC, 2008), continued

5) **COLLECTION, USE, AND DISCLOSURE LIMITATION**. Individually identifiable health information should be collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately

6) **DATA QUALITY AND INTEGRITY.** Persons and entities should take reasonable steps to ensure that individually identifiable 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

Legal, Privacy and Security

The 8 Principles (ONC, 2008), continued

7) **SAFEGUARDS**. Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure

8) **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

Policy and Operations Tiger Team

Policies and Documents produced:

- PA HIE-Network Privacy Policy P&P
- PA HIE-Network User Management Policy P&P
- PA HIE-Network Monitor-Audit-Breach Policy P&P
- Draft Notice Privacy Practices for HIE
- Draft Statewide form for Opt Out
- PAePA DURSA (between Community Shared Services (CSS) and Certified Participant(CP))
- PAePA BA Agreement (between CP and Member Organization (MO))
- PAePA MO DURSA (between CP and MO)

Policy and Operations Tiger Team

Electronic Sharing of Health Records Containing Super Protected Data (SPD):

- Ideal – Software/EHRs capable of sorting and segmenting SPD from the primary record, so that SPD is not improperly shared
- Current Compromise – expansion of the CSS Opt Out (Consent) Registry to include specialized SPD sharing permissions from patients who wish their SPD to be available for targeted sharing

HISP Certification

PA e HEALTH PARTNERSHIP AUTHORITY

HISP Operations/Certification

PA HISP Trust Community consists of any certified HISP that demonstrates ability to:

- Exchange secure, encrypted and authenticated emails using DIRECT specifications with other certified HISPs
- Ensures adherence to Authority requirements to protect PA citizens and their PHI

HIE Certification

PA eHEALTH PARTNERSHIP AUTHORITY

HIE Operations / Certification

- Certification program will be finalized based on details of CSS technical deployment
  - Certified participants (CP)
  - Member organizations (MO)
- Aligned with HIPAA, HITECH and commonwealth laws and regulations
- Security of information is of highest importance to Authority

Monitoring, Auditing and Breach Notification Policy

PA e HEALTH PARTNERSHIP AUTHORITY

Purpose of Policy

- Implementation of effective system auditing and monitoring practices to detect inappropriate access to PHI and hold accountable those who violate privacy requirements; and
- Compliance with Federal and state legal requirements for the reporting of privacy violations and security breaches to the appropriate entities and to affected individuals.

Scope of Policy

- The document applies to all Certified Participants connected to the Pennsylvania HIE-Network Community Shared Services (CSS), and their Member Organizations, Users and workforce members (as defined by HIPAA).

Scope, continued

- This policy is intended to be consistent with and does not replace or supersede any Federal regulations or laws (such as HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH)) or State privacy and security laws and regulations.

Objectives of Policy

- Define the requirements of the Authority and Certified Participants to establish policies and procedures for the auditing and monitoring of system transactions and ensuring accountability by attributing activities to individuals and enforcing consequences for privacy violations.

Objectives, continued

- Establish the responsibility of the Authority and Certified Participants to comply with Federal (HITECH) and State laws with regard to reporting and notification of a breach.
- Assign responsibility to the Authority to facilitate awareness and compliance with this policy.

Breaches

- All PHI incidents are now considered breaches, unless conclusively proven otherwise.
- *Old Standard*: Notification of breach was required only where “significant risk of financial, reputational, or other harm to individual”. Burden was on the covered entity or business associate to show there was no “significant risk”.

Breaches

- *New Standard:* Outside of certain existing exceptions, any use or disclosure of unsecured PHI in violation of the Privacy Rule is presumed a breach unless can demonstrate low probability that PHI has been compromised based on a risk assessment involving at least these factors:
  - Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification
  - Unauthorized person who used the PHI or to whom disclosure was made
  - Whether PHI was acquired or actually viewed
  - Extent of mitigation of risk to PHI

Breaches – Response Roles

- **Certified Participant and Member Organization**: Identify breach, notify Authority, notify affected persons, address security issue
- **Authority**: Preliminary investigation, action plan recommendations to Board, actions recommended by Board, follow up on any required action plans, possible HHS notification
- **Stakeholder CP Oversight Committee(s)**: Trust community action as to continued access of CP/MO to CSS or any other projected system or agreement impact

Breach Roles, continued

- **Board of Directors and Associated Committees:** Informed by Authority as to security incidents within trust community, any effects on CSS, will vote on any recommended response to incident that affects any entity access
- **HHS:** Will be appropriately notified when required by law or when recommended for notification

Breaches – PA Specific

Pennsylvania Statutes, Title 73 – Trade and Commerce

- Chapter 43 – **Breach of Personal Information Notification Act**
  - **§ 2302. Definitions.**
    "Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

Breaches – PA Specific, cont.

Pennsylvania Statutes, Title 73 – Trade and Commerce

- Chapter 43 – **Breach of Personal Information Notification Act**
  - **§ 2303. Notification of breach**. Notification made for each breach to affected person
  - **§ 2307. Notice exemption.** An entity that has established a notification policy as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance

Next Steps

- Finalize certification program
- Operationalize roles
- Monitor, learn and evolve

Questions?

For further information: www.paehealth.com

Alix Goss

PA Health IT Coordinator

Program Director

algoss@pa.gov

717-346-1115