

THSA



TEXAS HEALTH SERVICES AUTHORITY

Privacy and Security Workgroup *Facilitated Session II*

May 12, 2010

10:00 AM C.T.

Baylor Health Care System, Dallas, Texas

Agenda

- Welcome and introductions
- Subgroup findings: HIE policies and procedures
- Subgroup findings: State gap analysis
- Subgroup findings: Federal gap analysis
- Preparation for June 9 meeting
- Open discussion

Privacy & Security Workgroup

| Meeting #1 April 19: Austin | Meeting #2 May 12: Dallas | Meeting #3 June 9: San Antonio (tent.) | Meeting #4 July 14: Lubbock (tent.) |
|---|---|---|---|
| <ul style="list-style-type: none">▪ Introduce project and workgroup charter▪ Review survey results and core principles▪ Review deliverables▪ Discuss subgroups▪ Gap analysis between state and federal laws | <ul style="list-style-type: none">▪ Trusted network, oversight and accountability▪ Approach for managing trust agreements▪ Plan for modification for and recommendation of state laws | <ul style="list-style-type: none">▪ HIE training program: mindful and sensitive to patient information▪ Plan to address statewide policy and procedure based on workgroup outcomes | <ul style="list-style-type: none">▪ Case scenarios▪ Review and finalize deliverables |

Key Definitions

Privacy:

- Protection of individually identifiable personal health information

Security:

- Authentication, authorization, access, and audit

Master patient index:

- Patient matching when data is populated into the exchange and when the end user does a patient search

Consent:

- Informed permission for electronic exchange, need to record patient consent preferences to ensure that it continues to adhere to the patient's wishes

NCVHS definitions

Key Definitions, *cont.*

Health Information Organization (HIO):

- An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards

Health Information Exchange (HIE):

- The electronic movement of health-related information among organizations according to nationally recognized standards

[source: Funding Opportunity Announcement]

Key Definitions, *cont.*

ARRA (American Recovery and Reinvestment Act):

- Also known as the ‘stimulus bill;’ signed into law on February 17, 2009

HITECH Act (Health Information Technology for Economic and Clinical Health):

- A subset of ARRA which designates ~\$34 billion to help healthcare providers obtain meaningful use of HIT, including EHRs and care coordination through HIE

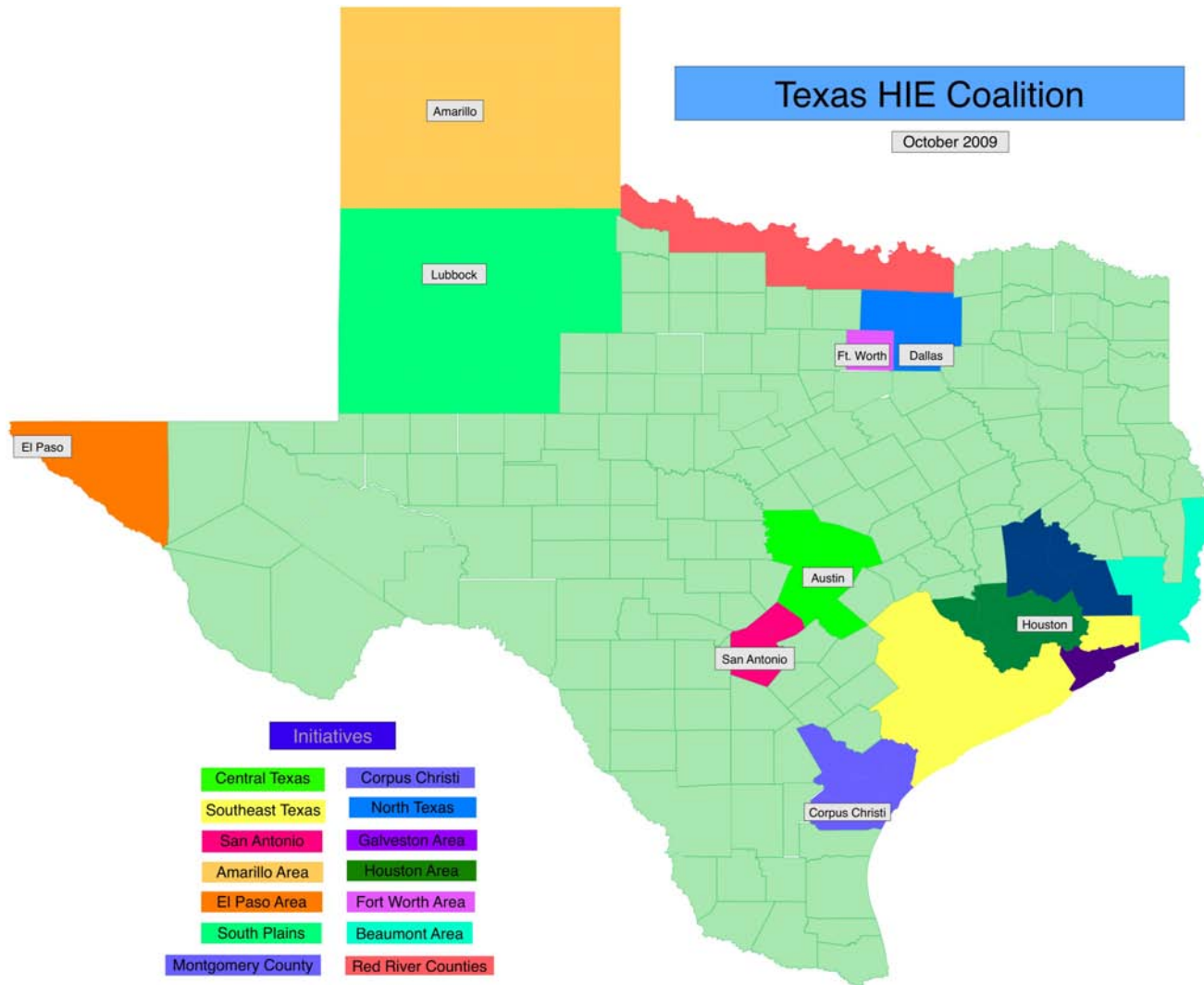
Meaningful use:

- Use of a certified EHR technology in a manner consistent with criteria including e-prescribing through an EHR, and electronic exchange of information for the purposes of quality improvement

Subgroup Findings:

HIE POLICIES/PROCEDURES

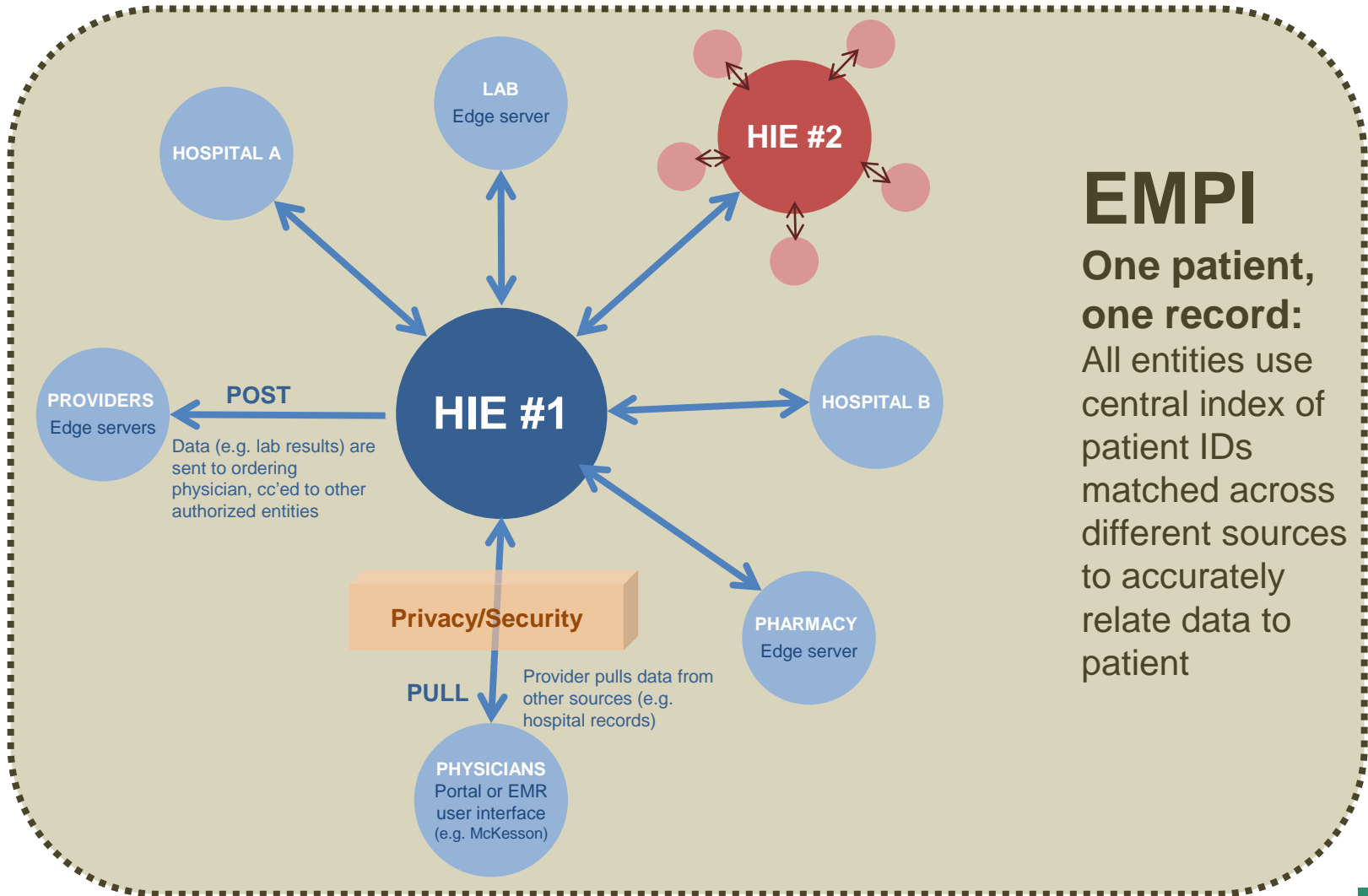
Existing Texas HIEs: Geography



Source: THIEC Needs Assessment 2009

Model for Exchanging Data

Inter- and Intra-HIE



Models for Sharing Patient Information

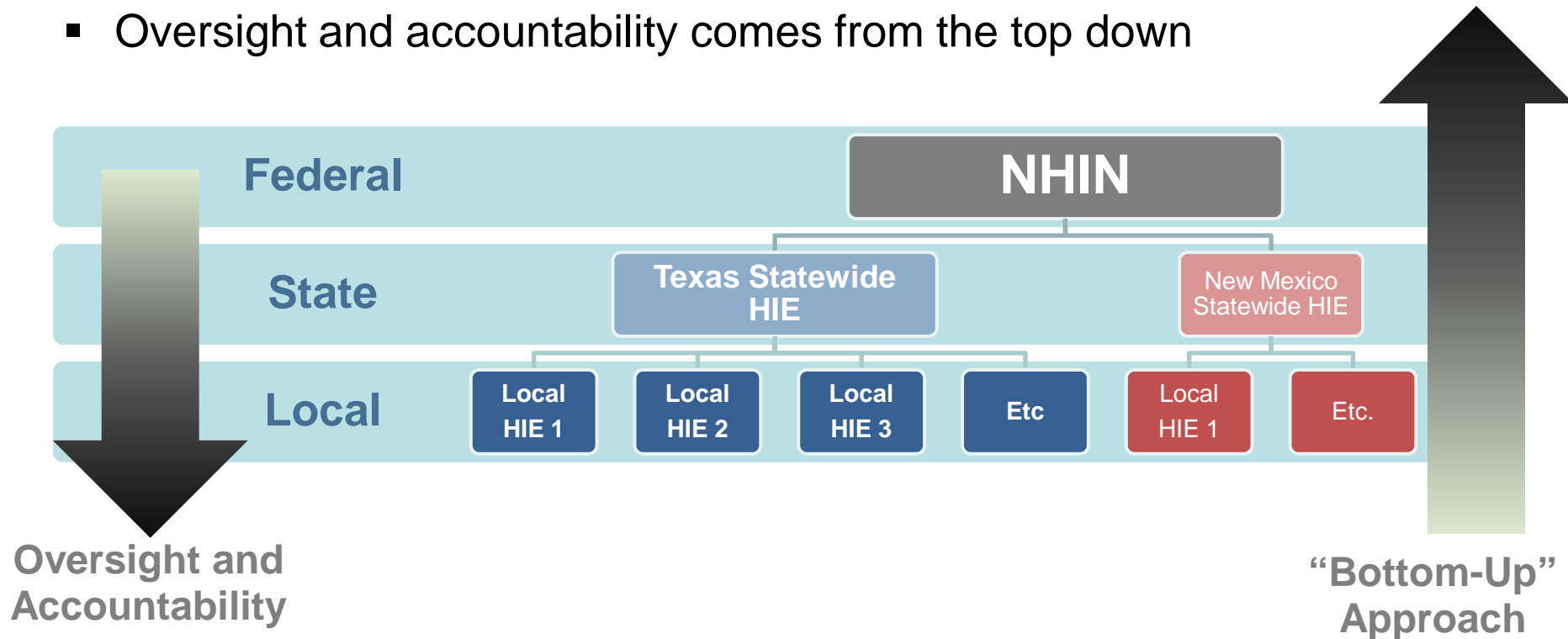
Local and State Levels

- **Data sharing:** Individually identifiable patient information
 - At the local level, data is used for **treatment**
 - Consent for data sharing must be ‘all or nothing:’ providers need complete information they can trust to appropriately treat patients
- **Data aggregation:** Non-identifiable patient information/quality measures
 - At the statewide level, data is used for **research and analysis**
 - Granular consent is permissible because quality of care is not affected

HIE Model

Network of Networks

- The Cooperative Agreement calls for a “network of networks” rolling up from the level of local HIEs, to statewide HIE, to federal NHIN
- Trusted network: Entities agree to participate/cooperate for the good of the community
- Oversight and accountability comes from the top down



HIE Privacy and Security

Basic Principles

- **Patient care and patient privacy:** Privacy must be delicately balanced against the need to access information to provide appropriate treatment
- **Security in an electronic world:** Heightened sense of vulnerability regarding identifiable health information in electronic form
- **Appropriate scope of disclosure:** There must be clear definition of who needs to see what information
- **Informed patient consent:** Consent must be meaningful, tracked, and monitored to earn patient trust in an HIE
- **Sensitive information:** Regulations governing specially protected health information vary at state and federal levels, presenting challenges for staff, education, and compliance
- **Patient control:** Create an environment that supports the consumer's right to control use of his/her personal health information

Subgroup Findings:

STATE GAP ANALYSIS

Privacy & Security

Texas State Laws: Current State

Goal

- Identify significant Texas state law issues affecting health information exchange within the state

Findings

- Texas state law mirrors HIPAA for the most part

Challenge

- Texas laws regarding privacy and security are currently scattered throughout legislation

Privacy & Security

Texas State Laws: Proposed Actions

- **Proposed (long-term) solution:** Streamline Texas laws related to privacy and security
- **Ongoing advisory role:** Create a privacy and security workgroup that will continue to evaluate and ultimately recommend a framework for privacy and security policy and procedures
- **Governance:** Develop and implement mechanisms for policy decision-making

Key Decision Points

- Decision-making entities will need to consider:
 - Key initial policies to incorporate at state level
 - Scope of information to be included (initially and long-term)
 - Who will have access?
 - Under what circumstances will access be granted?
 - For what purposes will access be granted?
 - At what level(s) will auditing take place?
 - Technology solutions that will enable these policies
- Create checklist of these considerations to guide decision-making entities in efforts that will follow

Subgroup Findings:

FEDERAL GAP ANALYSIS

ONC's Eight Principles for Nationwide Privacy & Security Framework

Eight principles of nationwide privacy and security framework for electronic exchange of medical information:

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use, and disclosure limitation
6. Data quality and integrity
7. Safeguards
8. Accountability

ONC's Eight Principles for Nationwide Privacy & Security Framework, *cont.*

| | ONC requirements | Considerations for meeting ONC requirements |
|--------|--|--|
| 1 4 | Individual access, Individual choice | <ul style="list-style-type: none"> ▪ Timely, simple means to access understandable, readable IIHI ▪ Informed consent: meaningful, tracked, monitored |
| 2 | Correction | Accuracy of individually identifiable health information (IIHI) |
| 3 8 | Openness and transparency, Accountability | <p>Participation agreement: Link between participants HIE network, wherein participants agree to:</p> <ul style="list-style-type: none"> ▪ Create and use a shared technology for HIE ▪ Follow common policies and procedures that enable HIE ▪ Accept specified consequences for failure to follow policies and procedures |
| 5 | Collection, use, and disclosure limitation | Collection and use of IIHI for specific purposes |
| 6 | Data quality, Integrity | <ul style="list-style-type: none"> ▪ Mechanisms ensuring that IIHI is current, accurate, precise ▪ Integrity: Data maintenance to conformity over time |
| 7 | Safeguards | Authentication, authorization, access, and audit |

Federal HITECH Requirements for all HIPAA covered entities

- Breach requirements (identification and notification)
- HIPAA and non-HIPAA (i.e., any organization holding personal health information) now protected
- Regional office privacy advisors/education initiatives for users of health information (local/state HIEs)
- Restrictions on sale of health information
- New accounting requirements for disclosure related to treatment, payment, and operations
- New access requirements for individual related to healthcare information electronic format
- New conditions for marketing and fundraising activities
- User de-identifiable data
- Minimum necessary data will be addressed
- Enforcement, improvement, and penalties increased

June 9, 2010

PREPARATION FOR NEXT MEETING

Privacy & Security Workgroup

Objectives for June 9 Meeting

June 9: San Antonio

- Objectives:
 - HIE training program: mindful and sensitive to patient information
 - Plan to address statewide policy and procedure based on workgroup outcomes
 - Patient consent
 - Trust agreements

July 14: Lubbock (tentative)

OPEN DISCUSSION



Thank you!