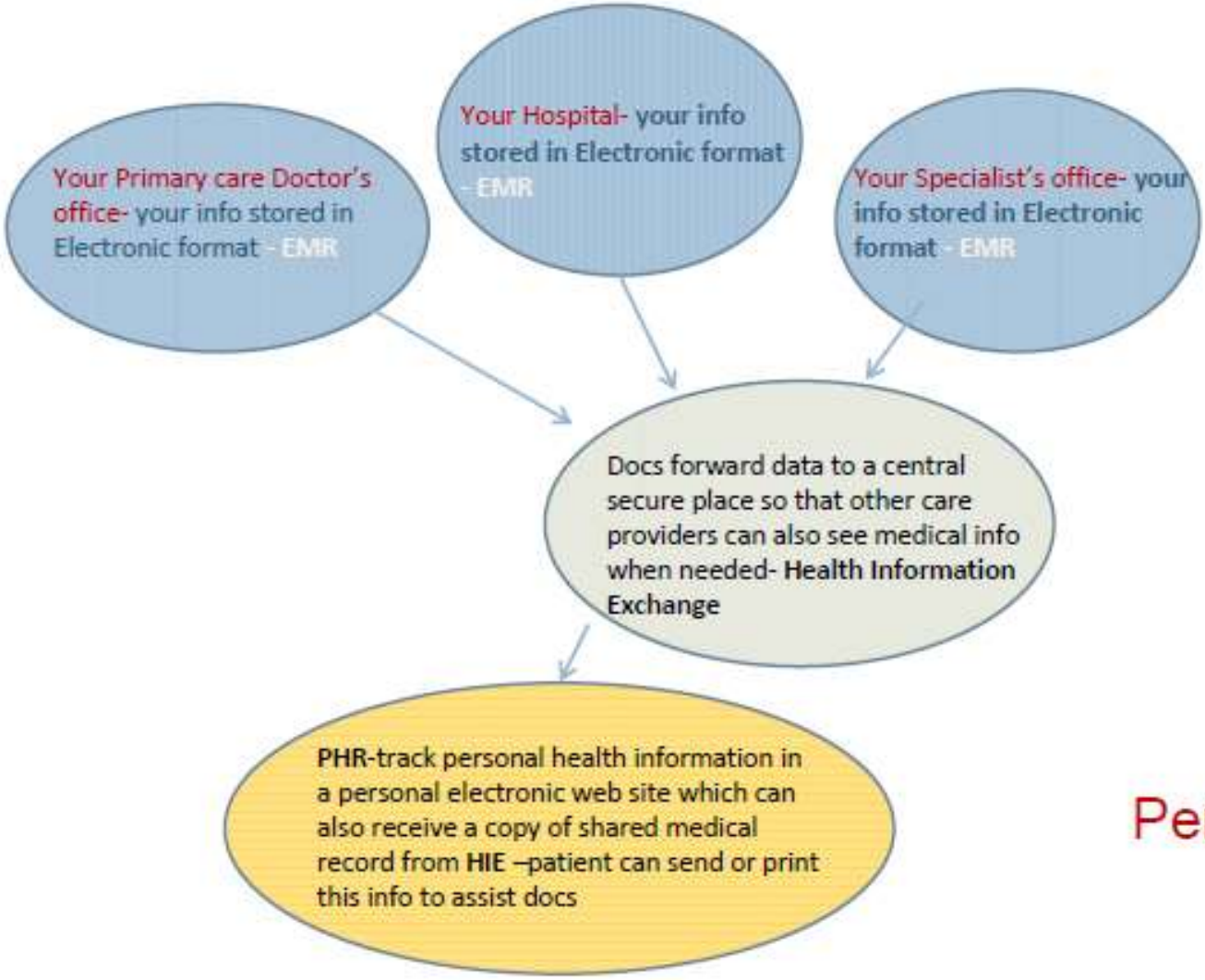
HIPAA Compliance and HIE

Andrew Lombardo, Director
Rio Grande Valley HIE
1413 Stuart Place Ste. B
Harlingen, Texas
Email: Andrew@rgvhie.org
Phone: 956.622.5801 Fax: 866-650-8035

How Electronic Health Information Works in the Community



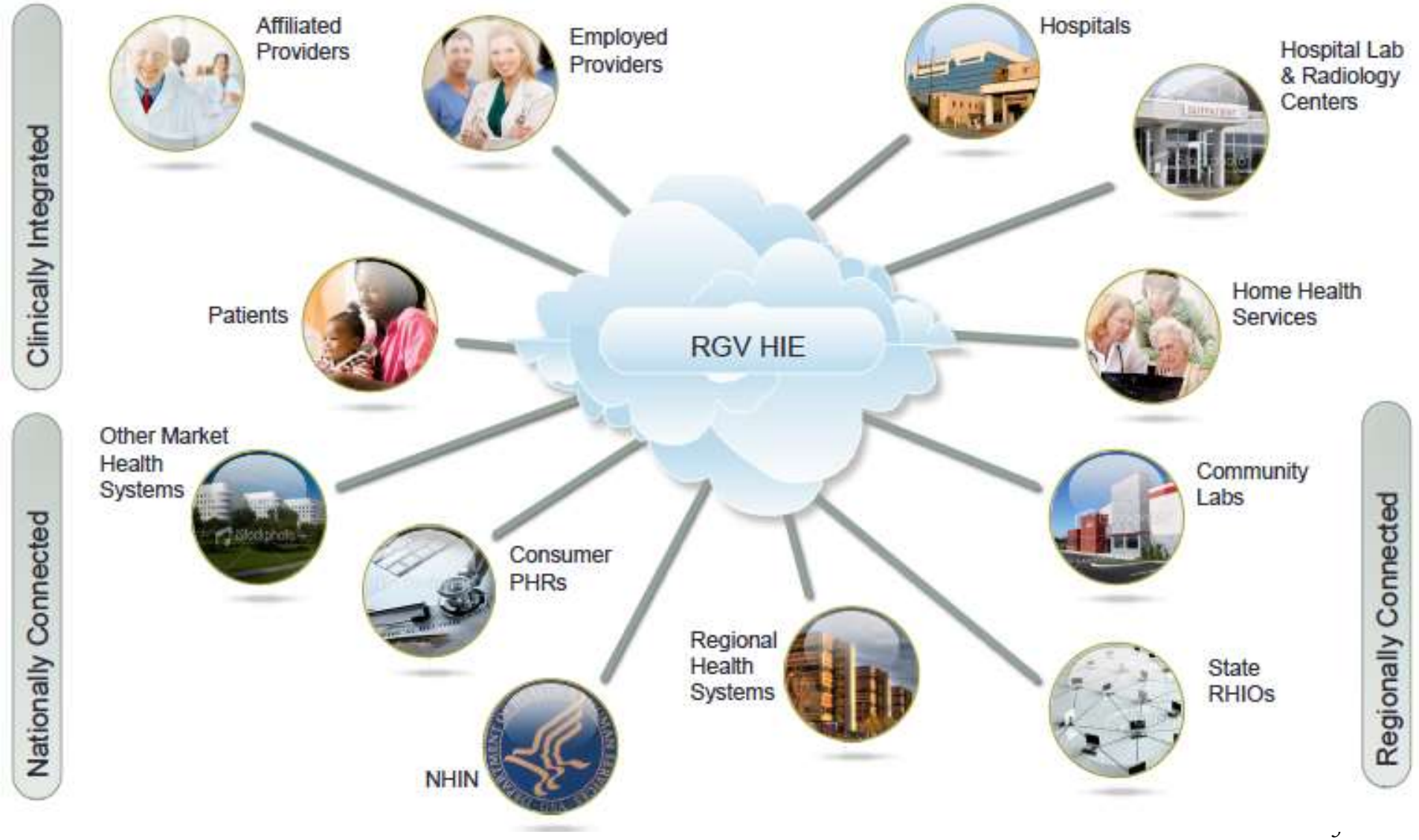
Electronic Medical Record

Health Information Exchange

Personal Health Record

Virtual Information Exchange Strategy

Extending Beyond the Clinically Integrated Health System



- Patient Longitudinal Health Record
- Clinical Messaging
- Results Delivery-Lab, Rad, Path, Discharge Summaries
- ED Care Alerts

Patient Longitudinal Health Record

Allows hospital to securely deliver results from their labs, radiology, pathology, transcription, and discharge systems to their ambulatory physician practices

Results Delivery

RGVHIE

Connected Results

Allows hospital to "push" HL7 feeds from their lab, radiology, pathology, transcription, and discharge systems to HIE

Optional

PHR

Allows patients to access their personal health information English and Spanish version available

Agenda

- Overview of State and Federal Law
- Opt Out Model: Provider Role
- HIE Agreements for Participation
- Required Policies and Procedures

Overview of State and Federal Law

- HIPAA and HITECH Requirements
- Guidance – ONC PIN 003
- State Law Requirements

Overview of State and Federal Law HIPAA and HITECH for HIEs

- HIPAA impact on HIEs
  - Privacy and HIEs
  - Security and HIEs
- HITECH impact on HIEs

Overview of State and Federal Law Guidance – ONC PIN 003

Individual Choice. Individuals should be provided a reasonable opportunity and capability to make informed decisions. . .

- PIN 003 states that patients have "meaningful choice":
  - Made with advance knowledge / time
  - Not used for discriminatory purposes or as a condition for receiving treatment
  - Made with full transparency and education
  - Commensurate with circumstances for why information is exchanged
  - Consistent with patient expectations
  - Revocable at any time

Overview of State and Federal Law
Key State Law Requirements

- Texas Medical Privacy Act
- State Privacy Laws for Sensitive Data (sample)
  - Genetic
  - Substance Use Disorder
  - Sexual Assault
  - Domestic Violence, child and elder abuse
  - Mental Health (other than psychotherapy notes)
  - Family Planning
  - HIV/AIDS/ Communicable Disease
  - Treatment of a Minor
  - Intellectual Disability

Opt Out Model – Provider Role

- Default - data is automatically exchanged; patients have opportunity to choose “opt out”, and not exchange data.
- Exception - sensitive data (e.g. HIV, substance abuse, etc) will not be exchanged unless patient consents.
- Providers obtain patient signatures when required. Provider or RGV HIE obtain signature on Opt Out Forms.
- RGV HIE provides sample language for authorization form and Notice of Privacy Practices.
- Providers establish procedures for collecting patient signatures which comply with PIN 003 Guidance for meaningful choice.

Opt Out Model – Provider Role High Level Steps

Patient Visit

- Patient given NPP
- Patient given Opt-Out Form if requested or referred to HIE to obtain form
- Patient given authorization form if required for sensitive data
- Data entered into EHRs by Provider; auth / opt out fields flagged if applicable

HIE Interface / HIE CDR

- Selected data elements sent to other providers through HIE
- Opt out and sensitive patient data either not sent or masked at HIE level as required
- Data stored in Database

Provider View

- View patient data
- Sensitive data available for view if authorization obtained where required
- Download data into EHRs or Print for paper medical records

HIE Agreements for Participation

- Business Associate Agreement
- Master Services Agreement
- Core Services Agreement

HIE Agreements for Participation
Business Associate Agreement

- Access to Information
- Notice of Breach Process

HIE Agreements for Participation
Master Services and Core Agreement

- Provider Key Operational Responsibilities
  - Superuser management of assignment and use of passwords to access information
  - Provide Superuser identifying information e.g. name, job title, department, supervisor, employee number or other identifier
  - Update information e.g. current users, deleting old users, adding new users w/i 48 hours of change in user status
  - Permit registration information to be audited
- Responsible for use, nonuse, interpretation of Health Data received, and accuracy of any Health Data sent

HIE Agreements for Participation
Master Services and Core Agreement

- RGV HIE Key Operational Responsibilities
  - Provide documentation and training sessions on how to access and use the services
  - Help Desk telephone support through RGV HIE's technology vendor
  - Secure, web-based access to technology platform and Core Services
  - Management of Opt-Out Form process, except when handled at Provider's Office

Required Policies and Procedures

- Patient Protections
- Security Risk Assessment

Required Policies and Procedures Patient Protections

- Right to an Accounting
- Right to Access and Copy
- Right to Amendment

Required Policies and Procedures Patient Protections – Right to Accounting

- Individuals have the right to ask and see information about who has seen their information (who looked up and who disclosed to)
- Applies once RGV HIE implements a database to store, assemble, or aggregate data
- Both RGV HIE's and the Participating Providers' Notice of Privacy Practices will inform individuals how to request an accounting
- Notice of Privacy Practices posted on RGV HIE website.

Required Policies and Procedures Patient Protections – Right to Access

- Individuals have a right of access (inspect and copy) PHI about them in the HIE
- Applies once RGV HIE implements a database – not initially
- RGV HIE Privacy Officer is responsible for responding to patient requests, at the direction of the Participating Provider's Privacy Officer

Required Policies and Procedures Patient Protections – Right to Amend

- Individuals have right to request corrections to their PHI and resolve disputes about information accuracy
- Applies once RGV HIE implements a database – not initially
- Provider who created the disputed record and provided the information is responsible for deciding whether to accept or deny the requested amendment.
- Individuals Informed by NPP posted on website.

Required Policies and Procedures Security Risk Assessment

- HIPAA Security Rules require HIEs to conduct a Risk Analysis
- Risk Analysis purpose is to assess and address potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI
- Risk Analysis conducted at least annually

Additional Information

- http://hietexas.org/resources/overview
- Primer - Medical Information Privacy Protections in Texas March 15, 2011, University of Houston Health Law & Policy Institute
- THSA Patient Privacy & Security FAQ (May 2013)