



TEXAS HEALTH SERVICES AUTHORITY

**THSA HIE Planning Engagement
Meeting Minutes
Privacy & Security Workgroup Meeting**

Date: 05/12/2010

Time: 10:00–11:30 am. C.T.

Location: Baylor Health Care System

2001 Bryan Street, CR-1, Dallas, Texas

Conference Call: (888) 276-8689 Access code: 5273822

Webinar: <https://www2.gotomeeting.com/register/798148978>

In Attendance:

Workgroup Members

Archie Alexander, MD, JD, LLM Health law attorney/mediator	Y	Michael Gerleman Availity	Y	Jennifer Reck Maximus	Y
Julian Armstrong, MD Sandlot, LLC	N	Patricia Gray U of Houston Law Center	Y	Edward Renteria, Jr. Blue Cross Blue Shield of Texas	Y
Sloan Cody Centene Corporation	Y	Charles Harrison Austin Travis Co. Integral Care	N	Diana Resnik Seton Family Hospitals	N
Kathleen Costello Texas HHSC	N	Derek Kang, MD Texas Children's Hospital	Y	Christy Rodgers Tenet Health System	N
Angelyn Estwick Texas DSHS	Y	Peter MacKoul, JD HIPAA Solutions	Y	Bud Thompson, MD	N
Lewis Ethridge Symantec	N	Pamela McNutt Methodist Health System	Y	Terry Turner Harris County Hospital District	Y
Susan Fenton, PhD Texas State University	N	Robert Myles Texas Health Resources	Y	Tracy Wade CHRISTUS/St. Michael Health	Y
Lorraine Fernandes Initiate Systems, Inc.	N	Deborah Peel, MD Patient Privacy Rights	Y	LaDair Wright Texas HHSC	Y
Celine Fynes Dell	N	John Quinn HL7/Accenture	Y		

Workgroup Staff/Observers

Taylor Cook Texas HHSC	Y	James Honn CTG	Y	Stephen Palmer Texas HHSC	Y
Mirsa Douglass Texas DSHS	N	Radhika Iyer CTG	Y	Liz Thelen CTG	Y
Tony Gilman THSA	N				

Other Attendees

Jim Campbell CTG	Y	Bob Hoover CTG	Y	Lynne Randall CTG	Y
Tomas Matthews PDX, Inc.	Y	Mitchell Gibbs Texas Health Institute	Y	Ann Kitchen THEIC	Y
Jim Hollester Texas HHSC	Y	Carolyn Witherspoon Coalition of Health Services	Y	Mark Butscher Symantec	Y
Kris Barton Galveston HIE	Y	John Wyand Squire Sanders & Dempsey	Y	Andrea Cobb Texas Medical Association	Y
Carole Tamayo ICC	Y	Lynn Moore PHNS/VBHS	Y	Joe Eberle CTG	Y



Agenda Items

#	Item Name	Item Owner	Time Allotment
1	Introductions Key Definitions	Radhika Iyer	10:00–10:10 a.m.

Discussion points:

- **Introduction:**
 - Goal of session is to decide on straw model for policy guidelines
 - To be consistent with the national privacy and security framework for electronic exchange of individually identifiable health information (IIHI), need to forge consensus on policies/procedures to protect privacy and security
 - Assure consumer engagement and adoption so patients have greater access to the protected health information communicated electronically with their providers to provide quality, affordability, and outcomes

- **Proposed definition of privacy: “Protection of individually identifiable personal health information”**
 - Under law (common law/case law, not statute), ‘privacy’ means individual’s right to control the acquisition and disclosure of private information, not protection of individually identifiable health information (IIHI)
 - It was suggested that NCVHS definitions should be considered and/or adopted
 - HIPAA does not include a single unified definition of privacy, was intended as a “floor;” stronger state, federal, ethical protections prevail

- **Proposed definition of HIE: “The electronic movement of health-related information among organizations according to nationally recognized standards”**
 - Focus on the movement of IIHI; movement of data needs to be protected
 - Definitions of HIE and HIO rely on nationally recognized standards; it is suggested that workgroup establish definitions that recognize the stronger protections in Texas state law
 - At federal level, meaningful use does not require EHRs be capable of segmenting special data (e.g. mental health, genetic, other sensitive conditions) but this is required by other states; if Texas does not require segmentation of data it will be unable to exchange with other states
 - Reason to adopt definitions proposed at the federal level is to prevent problems where entities can’t exchange data because differing definitions raise confusion as to whether data can be shared
 - Universal consent form that makes it clear to individuals what information can be released could eliminate data exchange hurdles even if definitions still vary slightly within the state
 - Few certified EHRs are capable of segmenting data

Participants: Radhika Iyer, Deborah Peel, Stephen Palmer, Peter MacKoul, Patricia Gray



2	Subgroup findings: HIE policies/procedures	HIE subgroup	10:10–10:30 a.m.
---	--	--------------	------------------

Discussion points:

- **Privacy/security policies and procedures used by Texas HIEs:**
 - HIEs’ policies are more strict than HIPAA, comply with state law and HIPAA
 - IIHI not viewable unless patient signs authorization form, authorization forms are HIPAA and state law compliant
 - Signed authorization is good for all provider members in the HIE, patient is given with information about who those members are
 - Exceptions for ‘break the glass’ situations (e.g., emergency room): data viewable by doctor without patient authorization, technology tracks who ‘broke the glass,’ purpose, date, etc.
 - In some HIEs patient data may be de-identified, included in database, and used for program evaluation analytics and research
 - Data is not sold by any Texas HIEs
 - HIE participants sign business associate agreements
 - Technical security provisions are in place to protect data
 - Diana Resnik suggests very rigorous controls for accessing data (from technical security and business process standpoints), regional/local HIEs have to be tightly managed
 - Purpose of sharing data at the local level: to provide central access to most reliable data for medical care and care coordination
 - Sharing data at the state level: purpose is not medical care so sharing should be subject to more stringent and very specific controls by patient (second level of consent)

- **Specific practices used by the Galveston HIE:**
 - All participating members set up DBA
 - Currently only exchange data for medical purposes/coordination of care, considering sharing information for research etc. in the future
 - Members opt in by signing release form
 - Does not allow data exclusion or member exclusion (if patient does not want some data available, none of their data will be shared across HIE)
 - Reason: providers have access to most reliable data and don’t question whether some information is missing

- **Mental health patient participation:**
 - Allowing all health information, including mental health, to be viewable by providers will exclude patients (e.g. mental health patients) who will be unwilling to cooperate
 - After Hurricane Ike, Galveston HIE focused on making sure patient information would be accessible by providers in other areas in case patients needed to seek care elsewhere
 - Galveston works with local MHMR (Texas Department of Mental Health and Mental Retardation) to identify appropriate information to share so a provider in another area can make informed treatment decisions

- **Treatment, payment, healthcare operations (TPO) exceptions to HIPAA:**
 - TPO exception is very wide and enables doctors or HIEs to release data without patient consent, some providers define “TPO” as “Send out anything to anyone any time”



- HITECH requires that healthcare providers using an EMR begin applying accounting of disclosures to TPO starting in 2011
- HITECH allows patients who pay out of pocket to block flow of their data for payment and healthcare operations
- Identity theft is also a concern

▪ **Risk assessment:**

- Latanya Sweeney, PhD* testified before the 21st Century Healthcare Caucus Roundtable (U.S. Congress)
- Sweeney analyzed proposed models for NHIN, declared them deficient in terms of usefulness of data exchanged and privacy, believes use of HIEs/NHIN will expand untrackable dispersal and use of PHI
- Sweeney proposed formal risk analyses of HIEs/HIOs and NHIN so lawmakers and the public can evaluate different HIE architectures/structures
- Sweeney also recommended using federal funds to analyze and perform risk analysis of different forms of HIEs/RHIOs in Texas so safer, better systems can be built
- * Visiting Faculty, Harvard University and MIT; Distinguished Career Professor of Computer Science, Technology and Policy and Director of the Data Privacy Lab, Carnegie Mellon University; GAO Appointee to the Privacy and Security seat of the Federal HIT Policy Committee
- Full text of testimony available at <http://patientprivacyrights.org/2010/04/latanya-sweeney-testifies-before-congress>

▪ **HIE model:**

- Bottom-up approach
- Cooperative agreement calls for ‘network of networks’ from local to state to federal
- Oversight and accountability comes from top down
- HIE model needs to be consistent with ONC standards—balance patient’s right/control to use personal health information vs. access to information for treatment purposes
- Rights to health privacy have been a longstanding part of Texas law, doctors don’t have a right to patients’ health information
- AHRQ focus groups and polls show that patients expect to be able to share data selectively
- Blanket consent may permit too much sharing (no patient control over where data goes), need dynamic consents that reflect patients’ rights and choices
- Protecting data patients have consented to share requires very strong security protections from a technical/business perspective
- Must have *informed* patient consent (requires training at patient–provider level)

Participants: Radhika Iyer, Ann Kitchen, Kris Barton, Patty Gray, Peter MacKoul, Deborah Peel

3	Subgroup findings: State gap analysis	State subgroup	10:30–10:50 a.m.
<p>Discussion points:</p> <ul style="list-style-type: none"> ▪ Findings: <ul style="list-style-type: none"> ○ Attorney General’s HIPAA pre-emption analysis of 2004 found that most Texas laws are not pre-empted by HIPAA ○ Need to agree on definitional terms and legal definitions for various terms ○ Laws regarding confidentiality, medical records, privacy are scattered throughout Texas law ○ Attorney General noted that to be effective, federal authorizations would have to include points from 			



Texas' (and other states') more stringent confidentiality laws

- Subgroup is working on a chart that identifies Texas laws affecting confidentiality of medical records, records retention, what employers are entitled to know, if employers require a drug test, etc.

▪ **Suggested solutions:**

- Bring law together and harmonize it
- Look at California's confidentiality of medical information act: addresses all providers, addresses HIPAA, provides penalties for misuse or unauthorized disclosure of medical information
- Create ongoing privacy/security workgroup to continue to advise on issues
- Create Chief Privacy/Confidentiality Officer to evaluate HIE policies, ensure enforcement, lead efforts to adapt/respond to technology changes
- Build systems that are very protective of confidentiality of medical information
- Create system that enables collection of patient safety information, adverse events information, interactions of medical treatments including mental health, etc.
- Look at Florida's release of information forms: 1) Blanket (explains what data will be released), 2) Piecemeal (select what data to share, very specific)

▪ **Benefits of sharing health data:**

- Public health benefits
- Prevention of issues such as in Galveston after Hurricane Rita: little redundancy of electronic medical data; patient information could not be accessed in Dallas
- Potential to readily identify drug interactions, treatment impacts on disparate populations, etc.

▪ **Authorization vs. consent:** Consent is more broad, authorization is specific

▪ **Segmentation technology:**

- Technologically problematic?
- Technology exists for EMRs to segment data, has been used in U.K. for years (patients can segment data, physician knows that something has been segmented but not what), U.S. vendors provide these clinical systems in the U.K.
- Possible solution: require technology for segmentation be implemented within some timeframe

▪ **Minimal necessary use:**

- Limits TPO
- Was intended so users of data could request only the information needed for a specific task (e.g. payer would ask for least amount of information to accomplish payment)
- Has been inconsistently defined/applied, many users ask for full records

Participants: Radhika Iyer, Archie Alexander, Patty Gray, Deborah Peel, Peter MacKoul, Ann Kitchen, John Quinn, Pam McNutt, Kris Barton



4	Subgroup findings: Federal gap analysis	Federal subgroup	10:50–11:10 a.m.
<p>Discussion points:</p> <ul style="list-style-type: none"> ▪ Accounting/audit trail: <ul style="list-style-type: none"> ○ Accounting for Disclosures Rule expected summer 2010: Office of Civil Rights (OCR) may require physicians to report <i>why</i> a record was accessed ○ Technology is already in place to see who accesses data, when, etc. (but not why) for every transaction ○ OCR may require HIEs to be able to provide complete 3-year accounting in patient-friendly English, may also establish penalties ○ In case of discrepancy, patient could file a complaint with the OCR ○ Once Interim Final Rule is established, OCR (at federal level) and Attorneys General (at state level) will be able to file actions ○ HIPAA has been used as ‘standard of care’ in negligence actions ○ There have been lawsuits resulting from failed internal business processes ▪ Authentication and business processes: <ul style="list-style-type: none"> ○ Authentication/access granted at several levels ○ Authentication tools used by hospitals have good audit trails; will HIEs have same high standard? ○ Business process rules and technology are in place to support authentication in HIEs ○ Can be issue with physician staff logging in as physician (liability is with the physician in this case) ○ There have been settlements resulting from negligence cases caused by failed internal business processes ○ At UTMB/Galveston, providers determine access level for staff, access management group reviews requests for access, a different group actually provides access (checks and balances) ▪ HITECH requirements for HIPAA-covered entities (TPO): <ul style="list-style-type: none"> ○ If patient pays cash, they can block the flow of the information ○ Narrow interpretation: insurance company is not notified if patient pays cash (only payment information is blocked) ○ Broader interpretation: patient can block flow of information for payment and healthcare operations ▪ Sale of data: <ul style="list-style-type: none"> ○ Vendors may sell patient data acquired from hospitals/providers ○ Vendor contracts should be more closely managed to prevent vendors from selling data ○ Supposed to be de-identified, but this is nearly impossible ○ Vendors will be considered covered entities under HIPAA and will be held accountable <p>Participants: Pam McNutt, Deborah Peel, Bob Hoover, Peter MacKoul, Archie Alexander</p>			



5	Open Discussion	All	11:15–11:30 a.m.
<p>Discussion points:</p> <ul style="list-style-type: none"> ▪ FDA: <ul style="list-style-type: none"> ○ Raised issue of medical data stored in places that may not be addressed (e.g. donor database, county jail, foster children, etc.) ○ Address possible gaps in state law including as many bases as possible ▪ Security: <ul style="list-style-type: none"> ○ Security measures must not be overlooked (required to join HIE) ○ Address functionalities of security that will define HIE privacy practices: application review, vulnerability management, risk assessments, disaster recovery, business continuity, federated authentication, etc. ○ Required issues <p>Participants: Patty Gray, Robert Myles, Radhika Iyer, Peter MacKoul</p>			

Next meeting of Privacy & Security Workgroup:

June 9, 2009

9:00 a.m.–11:00 a.m.

UHS Technical Center

Technical Conference Room

8131 Pinebrook Dr. (IH – 10 & Callaghan Rd.)

San Antonio, TX 78230

Possible subgroup meeting dates prior to June 9 will be sent to subgroup members.

