

HIPAA AND HIE INTERFACE

"TO BUILD AN HIE"

DAVID B. NELSON

- Cal OHII SME on HIPAA/HIE/Privacy
- Health Care Compliance Association (HCCA)
 - Privacy Committee and Privacy Academy Faculty
- SDSU Extension HIT Certification HIPAA SME
- Formerly
 - Privacy Officer County of San Diego
 - HIPAA Privacy/Security Officer for County of Yolo
- CISSP, CIPP/G, CHRC, CHPC
- Dave.Nelson@OHI.ca.gov
- 916-651-0423 (Not allowed to interpret the law for YOUR situation)

CAL OHII

- Office of Health Information Integrity (OHII)
- As an "office" under the Secretary of HHS in Agency, answers to the Secretary
- Charged with HIPAA compliance for ALL state departments
 - Direct Authority for Agency Departments
 - Aging; Child Support Services; Community Services and Development; Developmental Services; EMSA; Health Care Services; Managed Health Care (Managed Risk Medical Insurance Board); Public Health; Rehabilitation; Social Services; and State Hospitals
 - Indirectly for Departments outside the Agency

QUESTIONS

1. Are LEMSAs protected for receiving data from a covered entity as part of our California EMS Information System, for program monitoring, evaluation, and quality core measures?
2. And then is the LEMSA protected when they submit to the State database for state level monitoring and evaluation?
3. As we move into "real-time" EMS Health Information exchange from the Field (ePCR) to the Hospital, are there any requirements with must be met to accomplish this sharing of information?

CAL OHII

- I am not empowered to give legal advice.
- Interpretation of the law in a given situation could be interpreted as giving legal advice.
- However I can walk through the most relevant interactions between privacy/security regulations and an HIE environment.
- YOU have to recognize what applies.
 - Protected is out; Requirements I can do.

OUTLINE

- Not Just HIPAA for HIE
 - Other laws
 - Interaction between laws
 - Permitted use and disclosures (u/d)
 - Emergency and State Reporting
 - "Liability" Driver
 - Seizure from "may"
- Data Flow Structure
- Controls that MUST be in place
- **Assumption: Emergency Treatment and Mandated Reporting**

I'D LIKE A PAIR OF CHOCOLATE COLORED...

- White
- Dark
- Milk
- Semi-Sweet



- Belgian
- Dutch Processed
- Hershey's Special Dark?

YOU SAY HIPAA...

- Public Law 104-191 and the Rules
- 42 CFR Part 2
 - Federally Assisted Alcohol Drug Programs
- Civil Code 56 (CMIA)
 - Confidentiality of Medical Information Act
- Civil Code 1798 (IPA)
 - Information Protection Act
- Welfare and Institutions Code 5328 (LPS)
 - Mental Health Records

WHICH ONE DO I FOLLOW?

- Preemption
 - More Stringent "Rules"
 - To the PARTS, not as a whole
 - Example: CMIA says "date" for an Authorization; HIPAA says "date or event" = MUST USE DATE
- NONE BETWEEN FED REGS - HIPAA & 42 CFR PART 2 = Must comply with both
- RULE: Follow ALL until you can find an exclusion or Control to address the mandate!!!

PERMISSIBLE USE/DISCLOSURE

- HIPAA
 - Treatment, Payment, Other Business Operation (TPO)
- 42 CFR Part 2
 - Treatment and 10 exceptions - Some with HOOPS
- Civil Code 56 (Confidentiality of Medical Information Act)
 - Treatment and Payment (56.10(c)(14) "...specifically authorized by law...")
- W&I 5328
 - Treatment and limited uses/disclosure w/out an authorization
- ALL ALLOW:
 - Where Mandated by Law
 - Where "authorized" by individual



AUTHORIZATION

- CMIA = 13; HIPAA = 12; 42 CFR = 7
- Don't match exactly
 - "specific and meaningful descriptions" would be different for each service = multipurpose Auth risky
- Some preclude others
 - Contents do not match
- No compound Auths (some research exceptions)
- Administration a burden

AUTHORIZATION PITFALLS

- "Just in case" (in your back pocket)
 - Can't predict
 - "specific and meaningful" or "content"
- Expiration Tracking
 - 20 Year Auth unacceptable to Privacy Advocates = violates the spirit of the law
- Doesn't support human decision making such as "Minimum Necessary"
- Validity of Auth based on EHR content
 - HIPAA? CMIA? W&I 5328? 42 CFR?



TIES TO EHR PITFALLS

- EHR systems don't interact
 - Varying formats: date, number, name content
- Non-Computable Data Fields
 - Case Notes w/sensitive data, Rx for single use conditions, data under multiple mandates...
- Client Matching Difficult
 - How many elements???
 - Where's the "Individual Unique Health Identifier"?????
- "Client's Permission" registry
 - Problems similar to Validity of Auth

CONFLICT

- Everyone Wants HIE to happen
- Clear benefits
 - Better outcomes
- Clear Barriers
 - Regulation Silos (risk avoidance)
 - Industry Standards for EHR
 - Entity to entity controls vary (no one model)
- Emergency Service has LEAST Barriers

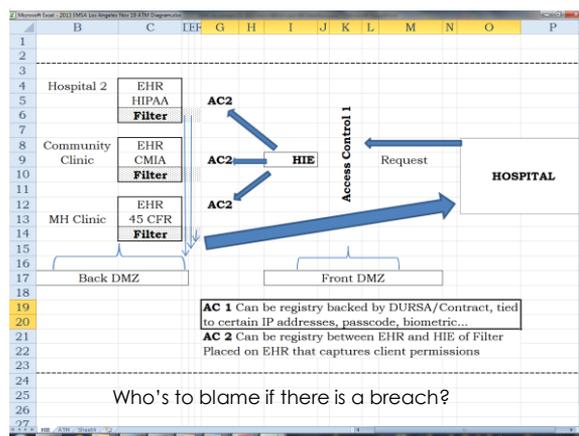
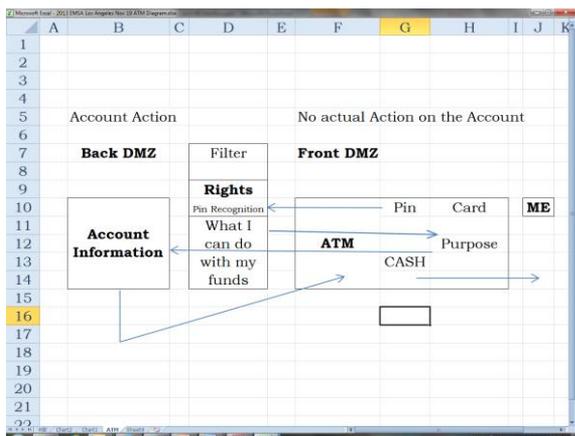
QUESTIONS??

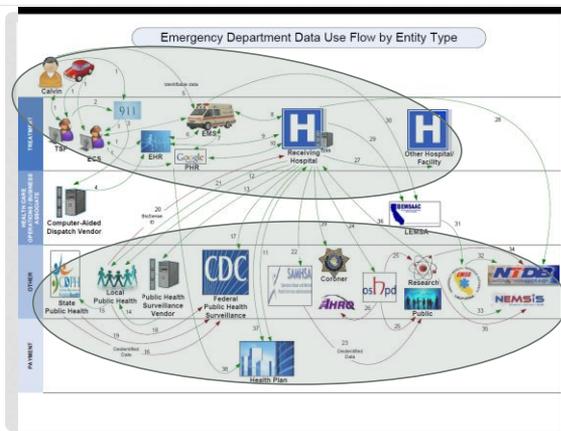


EMERGENCY & HIE



- Sorry, lots of detail!!!!
- Rollup into Comprehensive





EMERGENCY HIPAA

- "164.510 (b)(3) Limited uses and disclosures when the individual is not present
- ...if the individual is not present, or opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the CE may, in the exercise of professional judgment **1**, determine whether the disclosure is in the best interests of the individual **2** and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care **3** ... "

AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED.

- (j) Standard: Uses and disclosures to avert a serious threat to health or safety—(1) ... may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:
 - (i) (A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
 - (B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

NOTICE OF PRIVACY PRACTICE

- Right to Request Restrictions:
- If we agree, we will comply with your request unless the information is needed to provide you with emergency treatment as determined by your doctor

HIPAA HIE

- HIPAA
 - Use NPP to Notify Providers will U/D
 - In Emergency Circumstances
 - In the best interest of the individual
 - Limit the information to the situation (if possible)
 - No re-disclosure (retention ONLY for legitimate purposes)
 - Declare: Individual MUST notify if no U/D allowed in emergency
- Provides Opportunity for clinician to promote emergency U/D by declaring benefits and pitfalls of not permitting

42 CFR EMERGENCY

- 42 CFR 2.51 (a)
 - "...patient identifying information may be disclosed to medical personnel who have a need for information **1** about the patient for the purpose of treating a condition which poses and immediate threat **2** to the health of any individual and which requires immediate medical intervention." **3**

42 CFR HIE

- 42 CFR
 - Define how emergency request NEED will be determined
 - Authentication
 - Need classification or range
 - Documented Condition creating need
 - Documentation of immediacy conditions
 - Could tie to HIPAA NPP

CMIA EMERGENCY

- (c) A provider or health care service plan may disclose medical information as follows:
- (1) ...to providers of health care, health care service plans, contractors, or other health care professionals or facilities **1** for purposes of diagnosis or treatment of the patient **2**. This includes, in an emergency situation, the communication of patient information by radio transmission or other means between emergency medical personnel at the scene of an emergency, or in an emergency medical transport vehicle, and emergency medical personnel at a health facility licensed **3** pursuant H&S Code 1250) of Division 2...

CMIA HIE

- Determine
 - How will you know request is from permitted entity?
 - Document
 - How will you document requestor declaration that request is for Dx or Tx?
 - How will you document requestor licensure?

W&I 5328 EMERGENCY

- All information and records ...shall be confidential.
- (a) In communications between qualified professional persons in the provision of services or appropriate referrals, ...consent ... shall be obtained before information or records may be disclosed ... to a professional person **1** not* employed by the facility who does not* have the medical or psychological responsibility for the patient's care.
- ***Negatives**

W&I 5328 HIE

- Document
 - How do you know the requestor is a professional person responsible for the individual?

OUR HIE

- Clinician Uses NPP & Conversation to educate client (increases likelihood of client participation)
 - Capture exclusions of records
- System defines/document "need" for data
- System verifies/registers licensure and purpose
 - On File
 - National Enumerator for NPI – NOT verified
- System captures declaration of professional status and/or licensure
 - Attestation at Request

SAY WHAT?

- Questions should be:
 - Within an HIE framework what are the permissible U/D?
 - And
 - Within an HIE framework what can provider share for emergency services and state reporting
 - And
 - What Controls must be in place and supported
 - And
 - Where should the Controls reside?

PROVIDER ISSUES

- Holds individual's PHI
- Required to protect it (various regulations)
- Penalties go to
 - "unauthorized disclosures"
 - Not permitted w/out "authorization"
- Interpreted as:
 - W/out specific permission
 - Don't share unless you can afford the penalties
 - Decision may be at general staff

HIPAA SEIZURE



HIE CONTROLS

- Account for Laws apply to data & Provider
- HIE P&P may supplant local staff decisions
- HIE must reflect any
 - Restrictions known/identified/agreed to by provider
 - "My ex is an abusive EMT at John's Ambulance"
- EDUCATE HIE PARTICIPANTS ON
 - Who is providing each control
 - What each control addresses

QUESTION 1

- Are LEMSAs protected for receiving data from a covered entity as part of our California EMS Information System, for program monitoring, evaluation, and quality core measures?
- LEMSA's are entitled to receive the information and there is no prohibition or penalty associated with asking for the information. Penalties go to the holder if they do not use adequate safeguards in the submission.

QUESTION 2

- Is the LEMSA protected when they submit to the State database for state level monitoring and evaluation?
- Local to state falls under a permissive disclosure, as long as it is done securely.

QUESTION 3

- Are there any requirements that must be met to accomplish sharing of information in "real-time" EMS Health Information exchange?
- The submitting providers, and local LEMSA, may have to jump through some privacy and security hoops.

THANKS!

