



Legal Landscape for Health Information Exchange

HIE in EMS Summit
Tuesday, April 19, 2016

Presenter: Andrea Leeb RN, JD, CIPP/US

AGENDA

1. The Laws

- HIPAA/HITECH
- State Laws
- Sensitive Data

2. Consent Models

3. Contracts

1. The Laws

Which “general” laws cover the use and disclosure of medical information/protected health data?

The Grandparents

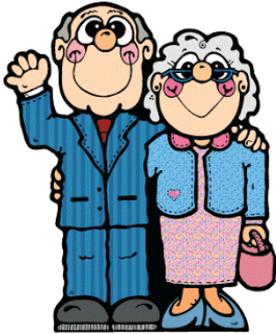


- HIPAA/HITECH
- CMIA

The Hipsters

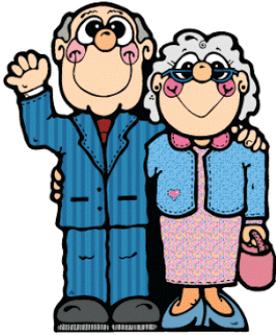


- AB1129
- AB503
- SB19



Health Insurance Portability and Accountability Act 1996

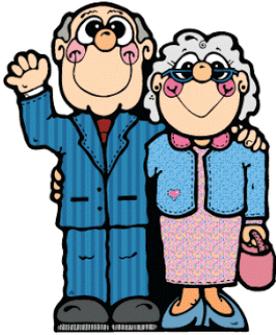
- The HIPAA Privacy Rule provides guidelines for how covered entities use and disclose protected health information.
- Generally, HIPAA restricts covered entities such as health plans and health care providers from using or disclosing an individual's information without his/her consent.
- HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, and was further modified by the Omnibus Rule in 2013.



Health Insurance Portability and Accountability Act 1996

QUESTION

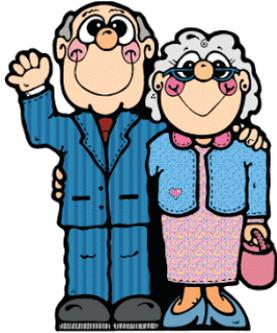
Does HIPAA require a covered entity to obtain member/patient consent prior to sharing or disclosing information with other covered entities through an HIE?



Health Insurance Portability and Accountability Act 1996

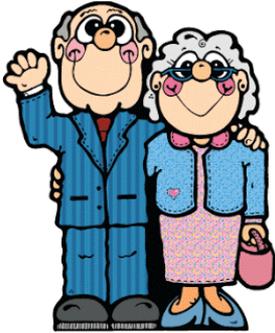
ANSWER: NO (mostly!)

- HIPAA does not create legal obstacles for sharing information through an HIE.
- This is because HIPAA contains exceptions that allow a covered entity to share information (without consent) for treatment, payment or healthcare operations.
- The primary exception under HIPAA is the sharing of psychotherapy notes.
- Note there maybe consent requirements under other federal or state laws for “Sensitive” Data.



Confidentiality of Medical Information Act

- Granddaddy of State Medical Privacy Laws
- CMIA is very similar to HIPAA
- Broad consent is permitted
 - Allows the exchange of most medical information and patient data for purposes of diagnosis and treatment without patient consent.
- There are more restrictions for certain “sensitive” data:
 - Behavioral Health
 - Substance Abuse



HIPAA vs. State Law

- HIPAA preempts state laws that permit disclosure unless the state law is “more stringent” than HIPAA
- “More stringent” means the law provides a higher level of patient privacy protection
- But HIPAA allows all disclosures **required by state law**



AB 503: Permission for Hospitals to Release PHI to EMS Providers, LEMSA, or EMSA

- AB503 was signed into law on 09/30/15 and became effective on 01/01/16.
- This law permits a hospital to release patient-identifiable medical information to an EMS provider, a local EMS agency, and the EMS authority, to the extent specific data elements are requested for quality assessment and improvement purposes.
- Purpose is to improve the quality of data shared between hospitals and EMS providers, thus improving the quality of care.



AB1129 – Data Formatting and Submission to Local Governing Agencies

- Signed into law on 09/30/15 and effective on 01/01/16.
- Requires EMS providers to collect and submit data electronically to their local governing agency in a format that is consistent with both prescribed state and national standards.
- Prohibits local governing agencies from mandating that EMS providers utilize a specific software package. Providers may use electronic record system that best meets their needs, provided the system is compliant with state and national standards.



SB 19 – POLST eRegistry Pilot

- Signed into law on 10/05/15 and the California Health Care Foundation is currently accepting pilot proposals until 04/29/16.
- This bill enacted the State Physician Orders for Live Sustaining Treatment (POLST) eRegistry Act to establish the POLST eRegistry Pilot, which will connect emergency health care professionals and other providers with patients' end-of-life care preferences to facilitate compassionate, desired health care during a crisis.
- The law provides the procedures to add information to the Pilot, subject to patient approval, and requires that POLST information be included in a patient's medical record.

“Sensitive” Data Laws

QUESTION

Are there special laws for certain kinds of patient data, such as behavioral or mental health data?





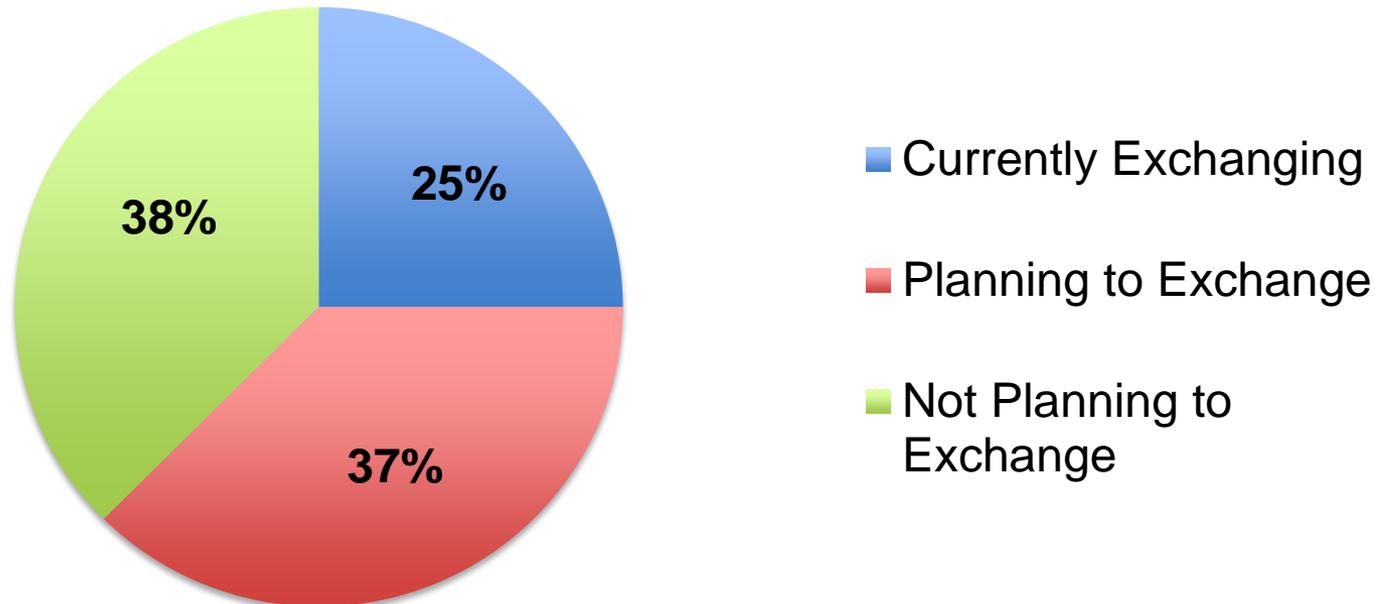
42 C.F.R. Part 2

- Governs confidentiality of drug and alcohol abuse treatment and prevention records.
- Currently requires explicit patient consent for a substance abuse record that obtained by (a) a federally assisted drug or alcohol program.
- Disclosure without consent permitted in a medical emergency.
- New Proposed Model Rules may allow for more general consent requirements to promote sharing of data--including sharing through an HIE.



HIEs Sharing “Sensitive” Part 2 Data

HIE Positions on Sharing Part 2 Data (2013)



Source: National eHealth Collaborative (NeHC) Survey of 135 HIE Initiatives, The Current State of Sharing Behavioral Health Information in Health Information Exchanges, September 2014, http://www.integration.samhsa.gov/operations-administration/HIE_paper_FINAL.pdf



California Health & Safety Code 11845.5

- Patient Consent required in order for providers to share a substance abuse record that is maintained in connection with substance abuse treatment efforts conducted or assisted by the California Department of Health Care Services.
- Patients must sign a written release that states the purpose of the disclosure.



California Lanterman-Petris Short Act

- Covers mental health information obtained by:
 - Federal, state, and county mental hospitals
 - Institutions that treat involuntarily detained patients
 - Residential programs and outpatient providers participating in government programs
- Limits disclosure without written consent to “qualified professional persons” who are exchanging information for treatment purposes.

2. Consent Models

QUESTION

Do HIE's need to obtain member/patient consent?





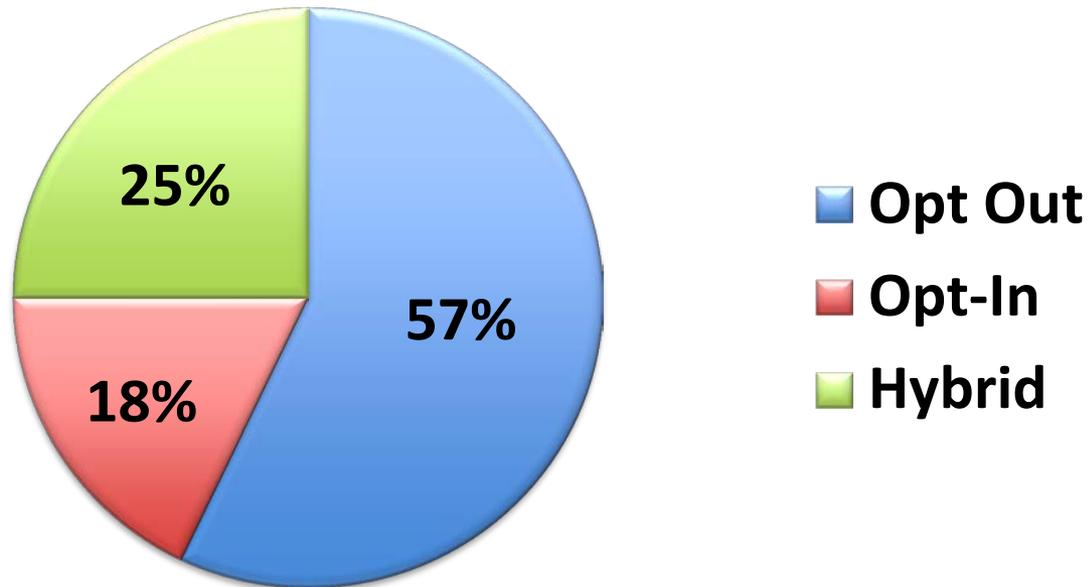
HIE Consent Models

- HIE Consent Models are either driven by state law or by the HIE's choice.
- **No Consent** - all patient data included; no opportunity to opt out
- **Opt-out Model** - all patient data included, but individuals can opt out completely
- **Opt-in Model** - patient data not included without individual's express consent
- **Hybrid** - combines opt-in and opt-out models



Use of Consent Models

NeHC Survey of HIEs (2013)



Source: National eHealth Collaborative (NeHC) Survey of 135 HIE Initiatives, The Current State of Sharing Behavioral Health Information in Health Information Exchanges, September 2014, http://www.integration.samhsa.gov/operations-administration/HIE_paper_FINAL.pdf



Meaningful Consent

- California law does not specify an explicit HIE consent model
- Office of National Coordinator for Health IT does not take position on HIE consent models, but advocates for a meaningful consent:
 - **Meaningful consent occurs when the patient makes an informed decision and the choice is properly recorded and maintained**
 - <http://www.healthit.gov/providers-professionals/meaningful-consent-overview>

3. Contracts

QUESTION

What kinds of contracts do covered entities need to consider before participating in an HIE?





Business Associates

- Covered entities are required to enter into business associate agreements (BAAs) with all vendors who use or disclose PHI on behalf of the covered entity.
- The BAA must contain certain provisions to ensure that the business associate protects PHI and complies with the requirements under HIPAA and HITECH.



Participation Agreements

- Each covered entity signs a separate agreement with the HIE
- Reflects the parties' shared understanding of roles, responsibilities and risks.
 - Including:
 - The participant's obligations to the HIE and other participants;
 - The permitted uses and disclosure of data;
 - The manner in which data will be accessed;
 - Data breach notification processes; and
 - Liability and indemnification provisions.



Federal DURSA

- **Data Use and Reciprocal Support Agreement**
- A comprehensive, multi-party trust agreement entered into by public and private organizations (eHealth Exchange Participants) that want to engage in electronic health information exchange
- The Federal DURSA is maintained by the Sequoia Project to support a nationwide exchange among HIOs and federal agencies.
- The Federal DURSA builds upon the various legal requirements that HIE participants are already subject to, and describes the mutual responsibilities, obligations and expectations of all participants.

Federal Consensus Among Parties

- The Federal DURSA reflects consensus among the entities involved in its development regarding many issues including:
 - Permitted Purposes for Use
 - Privacy and Security Obligations
 - Duties of Submitting and Receiving Participants
 - Use of Authorizations
 - Participant Breach Notification
 - Mandatory Non-Binding Dispute Resolution
 - Allocation of Liability Risk



CaIDURSA

- The California Data Use and Reciprocal Support Agreement (CaIDURSA) is multi-party trust agreement that allows all parties who have signed it to inter-operate using a common set of recognized standards.
- The CaIDURSA is compatible with the Federal DURSA, allowing organizations to be members both of the CTEN and eHealth Exchange.
- CaIDURSA is an important aspect of the California governance of inter-HIO data exchange over the California Trusted Exchange Network (CTEN).

QUESTIONS?

Contact Information:

Andrea Leeb

Chief Privacy Officer

Andrea.Leeb@calindex.org