

Health Information Exchange (HIE) Learning Series

HIE-103
Privacy and Security

11/17/2014

Cassandra McTaggart

Chief, Health Information Policy & Standards Division
Office of Health Information Integrity (CalOHHI)
California Health & Human Services Agency

Slide 1 of 43

November 17, 2014 - HIE Boot Camp

Acknowledgement

This course was originally developed for Planned Parenthood and funded by CalHIPSO from HITECH funds. The course is one of many educational materials produced by CalHIPSO in fulfillment of their role in educating stakeholders on health information technology.

CalEMSA expresses its appreciation to CalHIPSO for allowing it to use and modify the course content to fit the needs of this **HIE Boot Camp**.

Slide 2 of 43

November 17, 2014 - HIE Boot Camp

Course Overview/Purpose

The *Privacy and Security* course addresses the key issues that participants in health information exchange should be aware of, highlighting differences from the general requirements that all healthcare entities are subject to.

Slide 3 of 43

November 17, 2014 - HIE Boot Camp

Learning Objectives

At the conclusion of this HIE-103 course, participants will be able to:

1. Understand the importance of privacy and security in health information exchange
2. Describe a framework for understanding the variety of privacy and security requirements
3. Identify major federal and California regulations applicable to health information exchange
4. Lay out the key steps in assuring requirements are met.

Slide 4 of 43

November 17, 2014 - HIE Boot Camp

Course Outline

- Overview of Privacy and Security
- Privacy and Security Policy Framework
- Key Privacy and Security Requirements for Health Information Exchange
- HITECH Requirements
- Keys for Implementation
- Conclusion and Summary

Slide 5 of 43

November 17, 2014 - HIE Boot Camp

Course Objective #1

Understand the importance of privacy and security in health information exchange.

Slide 6 of 43

November 17, 2014 - HIE Boot Camp

Privacy & Security in HIE and the Networked World

Trust is built through repeated promises, delivery of results, and demonstrations of reliability.

- New Models of Care
- New Relationships among Partners and Patients
- New Technology
- New Obligations

Health Information Exchange

The electronic movement of health-related information among unrelated organizations according to nationally recognized standards in an authorized and secure manner

Interoperability



Patient-Centered Technology Ecosystem



Stakeholder Engagement



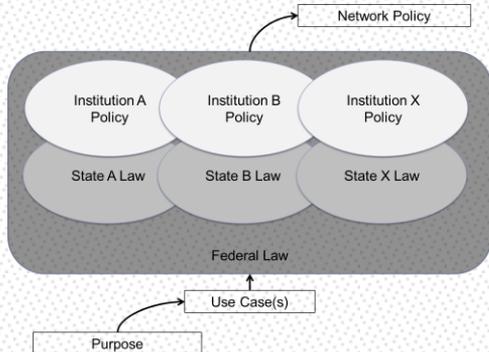
Course Objective #2

Describe a framework for understanding the variety of privacy and security requirements.

Privacy & Security Framework for the Networked World

- Potentially conflicting policies
- Many states haven't developed HIE regulations
- Where do you start?
- Who do you need to engage?
 - Analytical framework based on HHS HIE
 - Comparison of state/federal laws
 - Legal analysis summary

[Kim KK, McGraw D, Mamo L, Choo-Machado L.](#) Development of a privacy and security policy framework for a multistate comparative effectiveness research network. *Med Care*. 2013 Aug;51(8 Suppl 3):S66-72. doi: 10.1097/MLR.0b013e31829b1e9f.



Course Objective #3

Identify major federal and California regulations applicable to health information exchange.

State and Federal Privacy and Security laws

- The HIPAA Rules (45 CFR Part 160, 162, and 164)
- California's Confidentiality of Medical Information Act (CMIA—Cal. Civ. Code §§ 56 et. seq.)

Recent Federal Privacy & Security Regulations

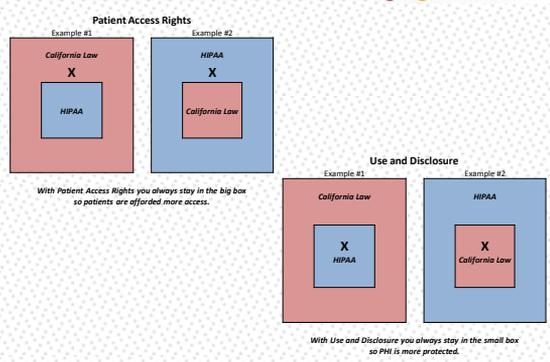
- HIPAA Omnibus Final Rule changes:
- effective March 26, 2013
 - compliance within 180 days by September 23, 2013
 - BAA's revised by September 22, 2014
- Health Information Technology for Economic and Clinical Health Act (HITECH), enacted February 2009
 - Genetic Information Nondiscrimination Act of 2008 ("GINA")

Preemption

- Preemption means determining which law applies and when.
- When state law and federal law conflict, federal law displaces, or preempts, state law, due to the Commerce Clause of the Constitution in this case.
- If Congress has not clearly claimed a regulation or law preempts state law, a federal or state court may examine legislative history as part of their analysis.

Note: If both laws can be complied with there is no preemption.

Preemption Examples



Patient Privacy

Primary issues

1. Authorization and Consent
2. Access to records
3. Right to amend
4. Breaches and accounting of disclosures
5. Business associates

Slide 19 of 43

November 17, 2014 - HIE Boot Camp

1. Consent and Authorization

Patient authorization not required under HIPAA and CMIA for use of PHI for:

- Treatment, Payment and Health Care Operations (TPO)
- Legal and administrative proceedings
- Public health reporting
- Research (Common Rule applies)

NOTE: HIPAA § 164.506, a covered entity may use or disclose PHI for TPO. Then goes on to say a covered entity **may** obtain consent of the individual to use or disclose PHI to carry out TPO.

* The use of consent and authorization is confusing because consent is used for treatment and authorization is used for uses and disclosures.

Slide 20 of 43

November 17, 2014 - HIE Boot Camp

Authorization for Sensitive Information

- HIPAA requires written authorization for the disclosure of psychotherapy notes, mental health, substance abuse
- The CMIA requires separate written authorization for disclosure of psychotherapy notes (Civil Code § 56.104)
- Other laws require written authorization for HIV test results (Health and Safety § 120975 et seq) and drug and alcohol abuse treatment (Health and Safety Code § 123105(b))

Slide 21 of 43

November 17, 2014 - HIE Boot Camp

HIO Consent (Permission)

- No federal regulations governing consent for electronic exchange of medical records through an HIO/HIE.
- HIPAA still applies to PHI being exchanged electronically by health care providers.
- HIOs must reconcile federal and state laws to ensure compliance before exchanging information.

Slide 22 of 43

November 17, 2014 - HIE Boot Camp

(Permission) Consent Models

- No consent
 - Treatment, operations, payment purposes only
 - Additional state requirements
- Opt-out
 - Greater participation rates
- Opt-in
 - Greater individual control
 - Technical limitations on granularity
- "Break the glass"
- CalOHII demonstrations project final report
<http://www.calohii.ca.gov/calohii/downloads/61-Demonstration%20Project%20Report.pdf>

Slide 23 of 43

November 17, 2014 - HIE Boot Camp

CalOHII Demonstration Project Findings

By evaluating consent through the Demonstration Projects, in conjunction with related activities conducted through the State HIE Cooperative Agreement Grant, CalOHII developed an assessment of what should be done based on the scope, as well as the constraints and challenges facing the industry. After an evaluation and analysis of the Demonstration Projects' findings, CalOHII recommends the following in order to advance the private and secure exchange of health information in California:

Slide 24 of 43

November 17, 2014 - HIE Boot Camp

Demo Project Continued



1. **Establish a common vocabulary and change the conversation** to reduce confusion with terminology, create a standardized language, and move away from patient permission as a single policy lever.
2. Continue to **let health information organizations determine the patient permission model** that is most appropriate for the community they serve.
3. **Patients must be provided an opportunity to make a meaningful choice** regarding the sharing of their protected health information.
4. **Technology solutions must evolve** to support granularity and electronic permission capture.
5. **Governance of interoperability is needed to sustain efforts.**

Slide 25 of 43

November 17, 2014—HIE Boot Camp

2. Access to Records



- Federal and California law entitle patients to receive copies of their health information, with some exceptions, such as for psychotherapy notes. (45 CFR § 164.524, CA Health & Safety Code, §§ 123100 et seq)
- Patients must ask providers for access to or copies of their records.
- Preemption analysis when state and federal law differ, comply with the law that provides greater access to patients

HIOs may be subject to access requirements only if they store records

Slide 26 of 43

November 17, 2014—HIE Boot Camp

Patient Access to Electronic Health Information



- If PHI held electronically, individuals are entitled to an electronic copy if in a "designated record set"
- Designated record includes:
 - Provider's medical, billing
 - Health plan's enrollment, payment adjudication, medical management
- Must be in the format requested if "readily producible;" or an agreed upon readable electronic form
- Not required to buy new software to do this
- If individual declines to accept electronic formats entity makes available, can default to hard copy
- Not required to accept patient's device – but can't require individuals to purchase a device from you

Slide 27 of 43

November 17, 2014—HIE Boot Camp

Patient Access to Electronic Health Information (cont'd)



- Must have reasonable safeguards in place to protect transmission of ePHI
- If an individual wants information by unencrypted email, entity can send if they advise the individual that such transmission is risky
- Must have a secure mechanism – can't force individuals to accept unsecure
- Up to 60 days (30 days less than previous rule allowed)

Slide 28 of 43

November 17, 2014—HIE Boot Camp

3. New Individual Right to Amend PHI



- Applies to PHI related to treatment decision making (e.g. not demographics) in a designated record set created by the covered entity
- May require written request (can be electronic) and reason (if this was previously included in the notice of privacy practices)
- Obligated to notify patient and business associate including HIOs and maintain amendments
- Written notice of decision within 60 days (with one additional 30 day extension)

HIOs are not required to support individual amendments

Slide 29 of 43

November 17, 2014—HIE Boot Camp

4. Breach Notification



- HITECH established right of individual to be notified of breaches of PHI
- Breach = An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates there is low probability that the PHI has been "compromised"
- Determining whether or not there is a low probability data has been "compromised" requires analysis of what happened (or may have happened) to the data
- Exceptions include inadvertent, good faith access or disclosures within a CE/BA if the data is not further subject to unauthorized use

Slide 30 of 43

November 17, 2014—HIE Boot Camp

Breach Notification - Risk Assessment

- CE/BA should perform risk assessment post-breach discovery and must consider at least the following:
 - Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification!
 - Who was the recipient of the PHI
 - Was the PHI actually acquired or viewed
 - The extent to which the risk to misuse of the PHI has been mitigated
- If no risk assessment performed, the default is notification
 - Burden of demonstrating low probability that PHI is compromised is on the CE/BA
 - Decision not to notify must be documented in case of review

HIOs are subject to breach notification requirements

Slide 31 of 43

November 17, 2014 - HIE Boot Camp

Accounting for Disclosures

Allowing individuals to know who has accessed their medical records brings the element of transparency to the right to privacy.

- California law does not require a provider to account for disclosures of health information.
- Prior to the HITECH Act, federal regulations did not require an accounting of disclosures for treatment, payment or business operations.
- account for disclosures of PHI for purposes of treatment, payment and business operations for three years prior to the date of the request.

HIOs must have audit capabilities

Slide 32 of 43

November 17, 2014 - HIE Boot Camp

5. Business Associates Regulations

- Expanded definition of "business associate", one who, on behalf of a covered entity, creates, receives, maintains or transmits PHI
- Subcontractors of business associates
- Contract between the covered entity's BA and subcontractors must satisfy the BA agreement requirements
- Based upon role and responsibilities, not whether contract exists
- HIOs are BAs
- Researchers are not BAs unless they are working on a covered entity's behalf

Slide 33 of 43

November 17, 2014 - HIE Boot Camp

Business Associates Regulations (cont'd)

- Must comply with some of Privacy Rule provisions and BAA
- Must comply with Security Rule
- Must conduct a risk analysis, implement a security awareness and training program, and appoint a security officer, among other requirements.
- BAs/subs subject to civil money penalties for HIPAA & HITECH violations
- Revised BAAs must be in place by 9/22/14

Slide 34 of 43

November 17, 2014 - HIE Boot Camp

Course Objective #4

Lay out the key steps in ensuring requirements are met.

Slide 35 of 43

November 17, 2014 - HIE Boot Camp

Steps for Meeting Requirements

- The best strategy to preserve information security is a culture of privacy
- Appoint privacy and security lead
- Conduct risk analysis
- Ensure BAAs are in place and compliant

Slide 36 of 43

November 17, 2014 - HIE Boot Camp

HIPAA Security Rule Risk Analysis

Requirement

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

Slide 37 of 43

November 17, 2014 - HIE Boot Camp

HIPAA Security Rule Risk Analysis

Questions

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain, or transmit.
- What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- What are the human, natural, and environmental threats to information systems that contain e-PHI?

Slide 38 of 43

November 17, 2014 - HIE Boot Camp

Technology and Security

How will you and your HIO handle:

- Data storage and backup
- Data transmission
- Encryption
- Data integrity
- De-identification or Anonymization
- Access control/authentication

Slide 39 of 43

November 17, 2014 - HIE Boot Camp

Elements of a Risk Analysis

- Scope: e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media
- Review Data Collection
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures
- Determine the Likelihood of Threat Occurrence
- Determine the Potential Impact of Threat Occurrence
- Determine the Level of Risk
- Finalize Documentation
- Periodic Review and Updates to the Risk Assessment

Slide 40 of 43

November 17, 2014 - HIE Boot Camp

Conclusion: Take Away's

- HIE opens up a new world
- Trust is paramount
- Educate yourselves on privacy and security requirements
- Privacy and Security in HIE requires
**Policy + Technology + Stakeholder
Engagement**

Slide 41 of 43

November 17, 2014 - HIE Boot Camp

Conclusion and Summary

1. Importance of privacy and security in HIE
2. Framework for understanding privacy and security requirements
3. Major federal and California regulations applicable to HIE
4. Key steps in assuring requirements are met

Good luck on successful HIE!

Slide 42 of 43

November 17, 2014 - HIE Boot Camp

Questions???

Cassie McTaggart

Cassandra.McTaggart@ohi.ca.gov