

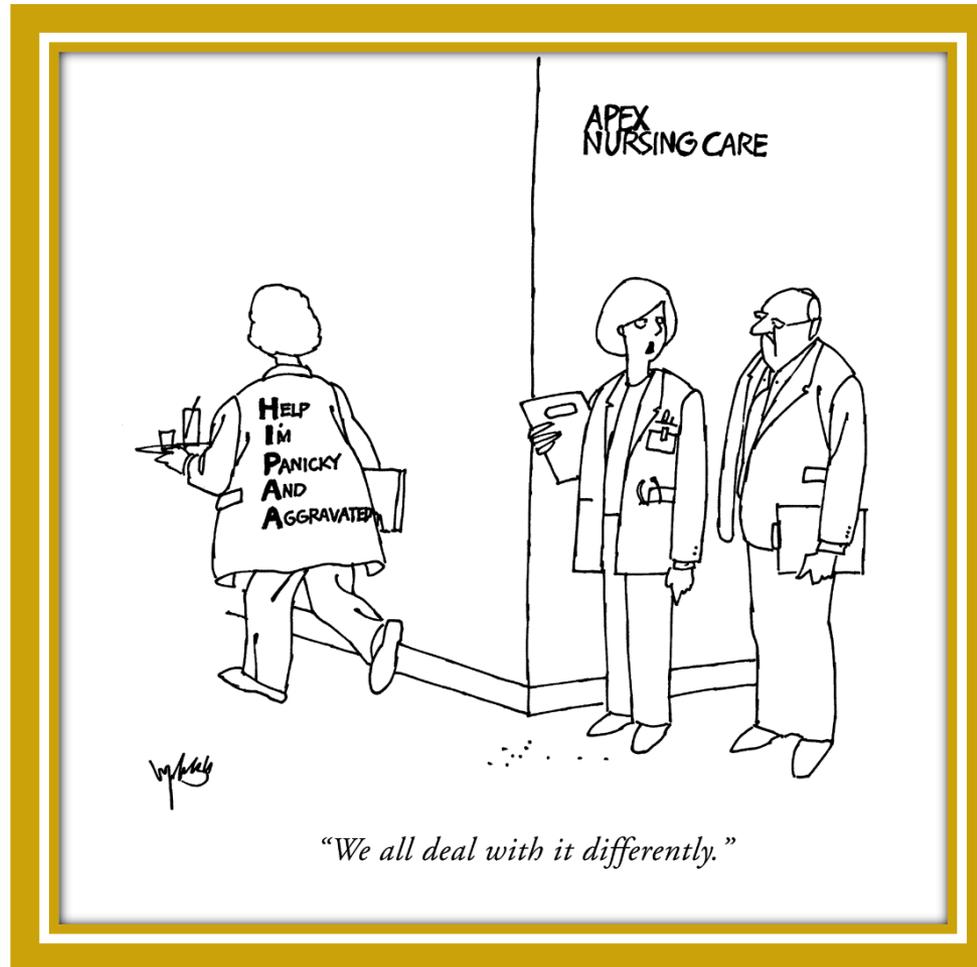


**Behavioral Health**  
**Office of Compliance**

**Behavioral Health  
Commission  
HIPAA  
Privacy and Security  
Training**

Marina Espinosa, MPA, CHC  
Chief Compliance Officer  
September 3, 2015





Source: Google Images

- By the end of this training, you will be able to:
- Summarize HIPAA Privacy and Security
  - Basics of HIPAA
  - Privacy Rule
  - Security Rule
- Compare and contrast HIPAA and State law
- Explain how Title 42, Substance Use Disorder, also addresses privacy
- Identify when an Authorization is needed
- Recognize potential breaches

- Health Insurance Portability and Accountability Act of 1996
- Federal Privacy Law: Title 45
  - Part 160: General Administrative Requirements
  - Part 162: Administrative Requirements
  - Part 164: Security and Privacy

- PII, IIHI and PHI
- Authorization
- Disclose without an authorization:
  - Treatment
  - Payment
  - Operations
- Safeguard information
- State law trumps if offers more privacy
- Business Associates

- Disclosures
  - Permitted uses or disclosures
  - Required disclosures
  - Prohibited uses or disclosures
- Minimum necessary
- De-identified PHI
- Notice of Privacy Practices
- Whistleblowers

- Privacy Officer
- Training
- Sanctions
- Mitigation
- Policies and Procedures
- Document
- Retain documentation

- Ensure confidentiality, integrity and availability of e-PHI
- Protect e-PHI against threat to security or integrity
- Protect e-PHI against uses or disclosures that are not permitted or required

## Administrative Safeguards

- Risk analysis
- Sanctions
- Security Officer
- Workforce clearance
- Security training
- Protection from malicious software
- Data back up
- Business Associate Agreement

## Physical Safeguards

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls
- Disposal
- Accountability

## Technical Safeguards

- Access Controls
- Unique User ID
- Automatic logoff
- Encryption
- Audit controls
- Integrity controls

- T/F: HIPAA is a federal law that has two (2) main parts :
  - 1) Administrative Requirements
  - 2) Security and Privacy

**False: HIPAA has 3 main parts to it: General Administrative Requirements, Administrative Requirements and Security and Privacy.**

- Does DBH have a Privacy Officer and if so, what is his/her name?

**Yes, it is Marina Espinosa.**



Source: Google Images

- Welfare and Institutions Code 5328
  - Specific to Mental Health
- Confidentiality of Medical Information Act
  - CA Civil Code, Sections 56 - 56.16
  - Regarding primary health

- More restrictive than HIPAA
- Can share without an authorization:
  - Treatment
  - Payment
- Tarasoff notification
- Abuse reports:
  - Child
- By order of the court

## **HIPAA**

### ***Comparable***

- Communication amongst treatment providers
- Communication regarding payment

### ***Differences***

- Disclosures about victims of abuse, neglect or domestic violence
- Use and disclosure for public health activities
- Judicial and administrative proceedings

## **W&I Code 5328**

### ***Comparable***

- Communication between qualified professional persons
- Communication regarding payment

### ***Differences***

- Disclosures about child abuse or neglect
- Disclosure to emergency response employee regarding possible exposure to HIV or AIDS
- Disclosure to the courts in the administration of justice

- T/F: HIPAA says federal law always trumps state law regarding privacy of PHI.

False: HIPAA has a provision that says if State law affords the client more privacy, it shall prevail.

- Provide one example of a disclosure that is the same in both HIPAA and CA law (WIC 5328).

Communication between treatment providers/qualified professionals OR  
Communication regarding payment



Source: Google Images

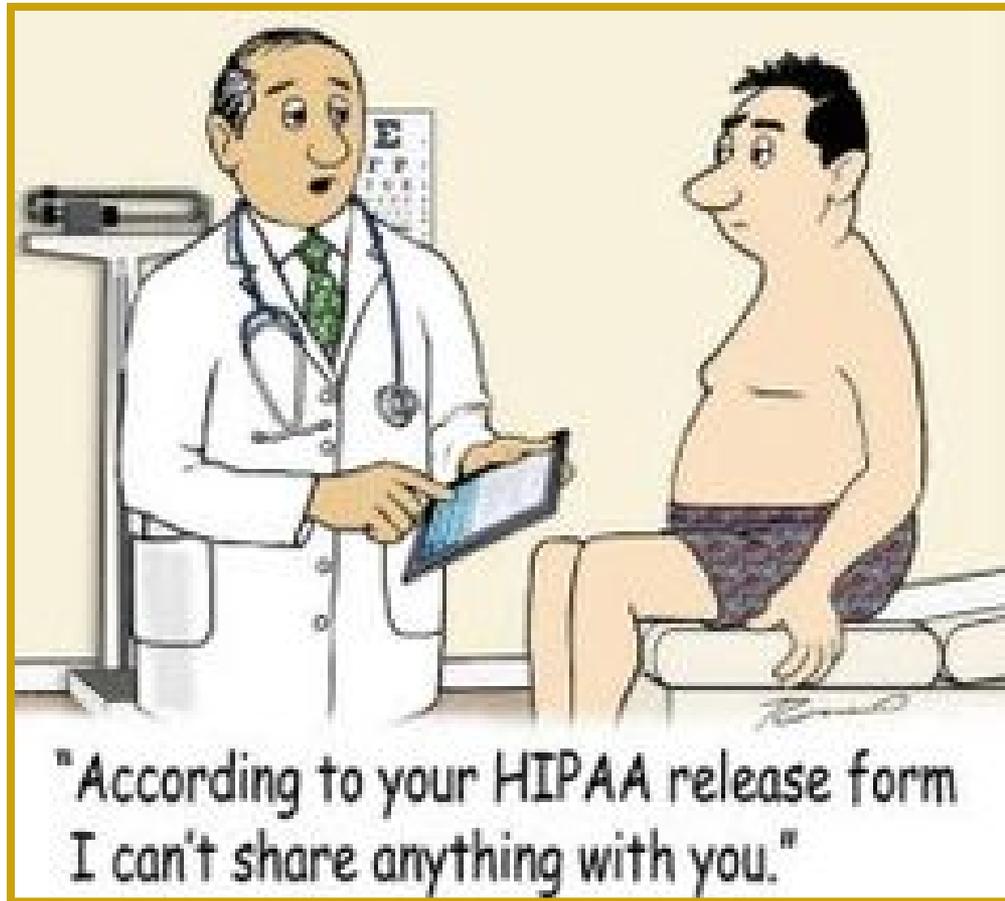
# Title 42: Confidentiality of Alcohol and Drug Abuse Patient Records

- Federal Law works in conjunction with HIPAA
- Need authorization to release any records, except the following:
  - Medical emergencies
    - To medical personnel to treat a condition that poses an immediate threat or requires medical intervention
    - To medical personnel of the Food and Drug Administration (FDA) who believe the individual may be threatened by a product under FDA jurisdiction
  - Research activities
    - Identity of clients will not be disclosed in the research results
    - Can only disclose client identifying info back to the program
  - Audit and evaluation activities
    - Restrictions on review of patient records
      - ✓ Can review but not copy or remove client records
      - ✓ Copy or remove but must destroy once audit complete
      - ✓ Can only disclose client identifying info back to the program

HIPAA: Health Insurance Portability  
and Accountability Act of 1996  
Title 45 Code of Federal Regulations  
Part 164

Welfare and Institutions  
Code  
Section 5328

Title 42 CFR  
Chap 1  
Part 2



Source: Google Images

- Per HIPAA, a client must have access to his/her records
- CA Health and Safety Code 123100 states the same, but there is an exception for mental health records
- Client shall receive copy within 5 working days after written request for record (unless more time is needed)
- *Important Note:* DBH retains the records of DBH contract agencies that are no longer in business

- Must follow state and/or federal laws when disclosing client information
- If there is not an exception to disclose PHI without an authorization, must obtain one
- When in doubt, DBH staff will get an authorization
- DBH cannot provide any information to anyone other than the client, unless there is an authorization or provision that permits. Examples include, but are not limited to, the following:
  - ❑ Parent of adult client
  - ❑ Parent of minor age 12 and up
  - ❑ MH advocate
  - ❑ BH Commissioner

- Title 42 allows PHI to be shared w/o an authorization in the following circumstances:
  - Treatment, Payment and Operations
  - Medical emergencies, Research activities and Audit and evaluation activities
  - Whenever and wherever you deem appropriate

**Medical emergencies, Research activities and Audit and evaluation activities**

- T/F: Even if I refer a person to DBH to obtain services, I do not have the ability to verify the person received assistance.

**True. Unless DBH has a signed authorization from the client stating you can receive info, DBH cannot confirm anything.**



- Not all incidents are breaches
  - Most are policy violations, such as, but not limited to, the following:
    - Sending an email containing PHI to the correct recipient but unencrypted
    - Sending email, send fax or initiate phone call containing PHI to incorrect DBH employee or DBH contract provider
    - Leaving encrypted laptop and other mobile devices unattended, resulting in theft



"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

Source: Google Images

- Information is disclosed that should not have been released...now what happens?
  - Incidents are evaluated to determine risk of compromise for client PHI
  - If determined to be a breach, the following will occur:
    - Client notification regarding breach including identifiers, mitigation, contact info, etc.
    - Department of Health Care Services notification
    - Department of Health and Human Services notification
- Examples of breaches:
  - Giving appointment card, discharge summary, letter, etc., to incorrect client
  - Giving prescription to incorrect client
  - Being unable to locate a medical record or chart note after an exhaustive search
  - Having an unencrypted laptop or mobile device and leaving it unattended, resulting in theft

- If a breach occurs, DBH notifies the following:
  - ❑ The client, Department of Homeland Security, Department of Health and Human Services
  - ❑ The client, Department of Health Care Services and Medi-Cal
  - ❑ The client, Department of Health Care Services and Department of Health and Human Services

The client, Department of Health Care Services and Department of Health and Human Services

- Provide 2 items that you learned in this training.

1.

2.

- ✓ Summary of HIPAA
- ✓ Differences of HIPAA and State law
- ✓ Identification of privacy law for Alcohol and Drug Abuse records
- ✓ Understanding when an Authorization to Release is needed
- ✓ Recognition of potential breaches



## *Office:*

- DBH Office of Compliance 909-388-0879

[Compliance Questions@dbh.sbcounty.gov](mailto:Compliance_Questions@dbh.sbcounty.gov)

- Marina Espinosa: 909-388-0882

[mepinosa@dbh.sbcounty.gov](mailto:mepinosa@dbh.sbcounty.gov)

- Linda Pry: 909-388-0881

[lpry@dbh.sbcounty.gov](mailto:lpry@dbh.sbcounty.gov)