SAN BERNARDINO COUNTY

Behavioral Health
Office of Compliance

# DBH Confidentiality, Privacy and Security Training

*Disclosures in Behavioral Health and CalAIM Data Sharing Information*

# HIPAA Privacy and Security




Source: Google Images

# Training Objectives



By the end of this training, you will be able to:

- Summarize Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security
  - Basics of HIPAA
  - Privacy Rule
  - Security Rule
- Compare and contrast HIPAA and State law, WIC §5328
- Explain how Title 42 Part 2 of the Code of Federal Regulations (CFR) addresses privacy of Substance Use Disorder (SUD) records
- Identify when an Authorization is needed for disclosure of PHI, for both mental health and substance use disorder PHI
- Recognize potential breaches and understand reporting procedures
- Know how to safeguard PHI to reduce likelihood of inappropriate disclosure

# Laws Governing Disclosure of PHI



The privacy, security and disclosure of PHI is governed by the following federal and state laws:

- **CFR, Title 45, Sections 160, 162 and 164, (Health Insurance Portability and Accountability Act or HIPAA):** Federal Law governs the confidentiality of both mental health and SUD client records.
- **California WIC, Section 5328:** State Law governs the confidentiality of only mental health client records (inpatient and outpatient).
- **CFR, Title 42, Part 2**: Federal Law governs the confidentiality of only SUD client records.
- **CA Civil Code, Sections 56.16**: Confidentiality of Medical Information Act (CMIA) (generally applicable for primary care settings, such as hospitals)

***Note:*** When there is a conflict between CMIA, WIC or 42 CFR and HIPAA the more stringent requirement is followed.

# Summary of HIPAA Regulation



Health Insurance Portability and Accountability Act of 1996

- Federal Privacy Law: Title 45 CFR
  - Part 160: General Administrative Requirements
    - Definitions like covered entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.
    - Preemption of state law
    - Compliance with the law
    - Complaint and investigations by Office of Civil Rights
  - Part 162: Administrative Requirements
    - Standard unique identifiers: National Provider Identifier (NPI) numbers
    - Requirements for HIPAA transactions
  - Part 164: Security and Privacy
    - Security standards such as swipe cards
    - Notification requirements in the event of a breach
    - Privacy standards such as positioning of computers or use of screen protectors

# HIPAA Basics



Definitions:

- PII- Personally identifiable information
- IIHI-Individually identifiable health information
- PHI-Protected health information:
  - PHI includes personally identifiable information (PII) such as name, address, date of birth, tied to past, present, or future health status, health care, or payment for health care, and is
  - Used, sent, or stored in any form, including paper, electronic, or verbal communications
  - Example: Individuals name + blood test results=PHI
- Authorization: Often referred to as consent, consent to disclose, release of information
  - An authorization allows for disclosing/using PHI as the client authorizes and instructs it to be disclosed or used
  - It also allows the client to limit the amount of PHI to be given, end the authorization at a designated time or stop as the client feels appropriate

# HIPAA Basics, cont'd.



- HIPAA allows the disclosure of PHI without client authorization for:
  - Treatment- between treatment providers
  - Payment- for services provided
  - Operations- such as compliance investigations, data collection, reporting to the State
  - A valid exception prescribed by law
- Safeguarding information- HIPAA requires providers/holders of PHI to implement Administrative, Physical and Technical safeguards to protect PHI, and to document these safeguards in policies and procedures.
- State law (WIC) takes precedence over HIPAA if it exceeds the privacy standard
- Business Associates- are held to the same standards and accountability for the liability of data breaches.

# HIPAA Privacy Rule Requirements



- Disclosures
  - Permitted uses or disclosures- Treatment, Payment, Operations (TPO) and other required disclosures/exceptions as required by law.
  - Required disclosures or exceptions- public health activities (reporting of disease), abuse reporting, or response to judicial proceedings.
  - Prohibited uses or disclosures- an Authorization to Release PHI is needed for any purpose other than TPO or an exception allowed by law as described above.

- Minimum Necessary Rule
  - The HIPAA Privacy Rule *Minimum Necessary Standard* limits the extent of access to and/or disclosure of protected health information (PHI) to the minimum amount of information provided to the minimum number of recipients necessary to accomplish the intended purpose or function.

# HIPAA Privacy Rule Requirements, cont'd.



- De-identified PHI
  - Requires all 18 identifiers on HIPAA List of Identifiers be removed.
- Notice of Privacy Practices (NOPP)
  - Clients have a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity and of their rights and the covered entity's legal duties with respect to PHI.
- Whistleblowers
  - HIPAA prohibits retaliation or intimidation against anyone filing a complaint.

# Privacy Safeguards



- Privacy Officer
- Training
- Sanctions
- Mitigation
- Policies and Procedures
- Documentation
- Retention of Documentation
- Oath of Confidentiality

# Oath of Confidentiality



DBH IN 17-11: Confidentiality Statement Requirement for Safeguarding PHI

- As San Bernardino County's designated Mental Health Plan (MHP) and Drug-Medi-Cal Organized Delivery System (Substance Use Disorder Administrator), DBH is responsible for ensuring the privacy and integrity of client records.
  - This responsibility includes the requirement to obtain reasonable assurances from individuals and entities to which PHI is disclosed that PHI will remain confidential and to implement administrative safeguards that protect the confidentiality, integrity and availability of PHI.
  - Per DHCS contract requirements, DBH is responsible for imposing the same restrictions and conditions on its contract providers. Thus, it is required that all DBH personnel, DBH contract staff, and any external entities reviewing DBH and/or DBH contractor client records (for the purpose of performing job-related duties, research, monitoring/auditing, and/or any other business operation) sign a confidentiality statement, also known as an "Oath of Confidentiality".
    - Oath of Confidentiality must be signed by all DBH and contract personnel at hire/start of contract and *annually* thereafter.

# Security Rule



The HIPAA Security Rule:

- Ensures confidentiality, integrity and availability of e-PHI
- Protects e-PHI against threats to security or integrity
- Protects e-PHI against uses or disclosures that are not permitted or required
- Prescribes breach reporting requirements (including reporting to impacted individuals within **60 days** of breach confirmation)
- Examples:
  - Policies and procedures that are put into practice, such as badge access to facility, requiring visitors to be escorted in areas where there is PHI, and securing PHI in locked areas when unattended.
  - Protection against threats to security/integrity by having servers located with the County Information Services Department, encrypted drives, firewalls, etc.
  - Protection against uses or disclosures not permitted or required – "Minimum Necessary" Rule; access to PHI only to perform job function, not allowing access to PHI on non-County devices, encryption on all used devices, etc.
  - Conducting a Risk Analysis - an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the department.

# Security Safeguards



## 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

# Privacy Officer



- HIPAA requires designation of a Privacy Officer:
  - **Privacy Officer** is responsible for implementation of a privacy program within an organization, which includes ensuring:
    - Privacy policies and procedures are in place to assure confidentiality of PHI
    - Effective training and education regarding privacy practices
    - Investigation of incidents in which a breach of PHI may have occurred, including research and risk assessment
    - Breach reporting, and ensuring client rights in accordance with state and federal laws (i.e., state/federal reporting, as well as client reporting within 60 days of determination)
    - Privacy risk assessments are conducted in regular intervals

**Privacy Officer**
Erica Ochoa

**909-388-0882**
eochoa@dbh.sbcounty.gov

# Security Officer



- HIPAA requires designation of a Security Officer:
  - **Security Officer** is responsible for ongoing management of information security program within the organization, which includes ensuring:
    - Security policies, procedures are in place for the protection and integrity of e-PHI
    - Adequate understanding and education of the safeguards required under the Security Rule, most specifically technical safeguards
    - Mechanisms in place to prevent unauthorized access to PHI (i.e., technical security controls)
    - Audit controls, such as system security review, log review, change control systems, etc.
    - Business Continuity and Disaster Recovery Plan

**Security Officer**
Rick Shackelford

**909-388-0910**
rshackelford@dbh.sbcounty.gov

# HIPAA and California State Law




Source: Google Images

# California Privacy Laws



- Welfare and Institutions Code (WIC) 5328
  - Specific to mental health for either voluntary or involuntary recipients of services
- Confidentiality of Medical Information Act
  - CA Civil Code, Sections 56.16
  - Pertains to primary health, and most generally governing privacy law for hospitals (non behavioral health services)
- Example of differing requirements:
  - California Confidentiality of Medical Information Act (CMIA) contains a provision stating we shall provide information to the coroner's office; WIC 5328 does not allow without consent.

***Note:*** HIPAA also allows for this disclosure *however* when determining the applicable law for the given setting and records, and most stringent law prevails.

# WIC 5328 Disclosure Without an Authorization



WIC 5328 allows for sharing PHI without an authorization for:

- Treatment-in communications between qualified professionals in the provision of services, appropriate referrals or conservatorship proceedings;
- Research in accordance with designated rules for the conduct of research;
- To a business associate or for health care operations purposes, in accordance with Parts 160 and 164 of Title 45 of the Code of Federal Regulations (HIPAA-case management and care coordination)
- To the extent necessary for a recipient to make a claim, or for a claim to be made on behalf of a recipient for aid, insurance, or medical assistance to which the recipient may be entitled;
- Tarasoff notifications;
- Child Abuse reports, and
- By order of the court

# Compare and Contrast Allowable Disclosures



## HIPAA

***Comparable***

- Communication amongst treatment providers
- Communication regarding payment
- **Treatment, payment health care operations**

***Differences***

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

## WIC 5328

***Comparable***

- Communication between qualified professional persons
- Communication to make a claim for aid, insurance, or medical assistance
- **Between business associates *or* for health care operations in accordance with HIPAA (45 CFR 164.501)**

***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

# Description of Treatment, Payment and Health Care Operations



**Treatment:** provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

**Payment**: activities to obtain payment or be reimbursed for services and of a health plan to obtain premiums and fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. Common examples include:

- Determining eligibility or coverage and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing medical necessity, coverage, charge justification, etc.;
- Utilization review activities.

**Health care operations**: administrative, financial, legal, and quality improvement activities of a covered entity such as DBH that are necessary to run its business and to support the core functions of treatment and payment. Summarized under 45 CFR 164.501, and may include:

- Quality assessment/improvement activities, population-based activities, case management and care coordination;
- Review competence and performance, training., accreditation, certification, licensing and credentialing activities;
- Medical review, legal, auditing, fraud and abuse detection and compliance program functioning;
- Business planning and development (i.e., cost management and analysis, etc.);
- Business activities and general administrative activities.

# 42 CFR Part 2 - Privacy Law Governing SUD PHI




Source: Google Images

# Brief History of 42 CFR Part 2



- In 1975, 42 Code of Federal Regulations (CFR) Part 2 was enacted to address concerns about potential use of substance use disorder (SUD) information in non-treatment-based settings, such as administrative and criminal hearings related to the patient.
- Intended to ensure that a patient receiving treatment in a Part 2 program does not face adverse consequences in criminal or domestic proceedings.
- Protects the identity, diagnosis, prognosis or treatment records of any patient maintained in connection with the performance of any program or activity relating to SUD education, prevention, training, treatment, rehabilitation or research, which is conducted, regulated or directly/indirectly assisted by any department or agency of the United States.
- Regulations have been updated multiple times over the past 50 years, including most recently (February 2024) and have been at the cornerstone of addressing concerns that discrimination and fear of prosecution deter people from accessing SUD treatment.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2 –Description



- **Federal Law protections for PHI created in a Substance Use Disorder (SUD) program:**
  - Applicable when PHI is created and/or disclosed by a Part 2 program: A Part 2 Program is a program in which an individual or entity is federally assisted and holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment.
  - If PHI did not derive from a Part 2 program, or is not being disclosed by a Part 2 program, it is **NOT** governed under Part 2
  - Simply because a substance use disorder is notated in the mental health record does not warrant protection under 42 CFR Part 2, the medical record must be derived within the SUD-Part 2 program to be protected under Part 2.
- **Need client consent (authorization) to release any records, except when the following applies**:
  - 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

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, cont'd.



- Audit and Evaluation Activities §2.53(c):
  - (1) Activities undertaken by a federal, state, or local governmental agency, or a third-party payer entity, in order to:
    - (i) Identify actions the agency or third-party payer entity can make, such as changes to its policies or procedures, to improve care and outcomes for patients with SUDs who are treated by Part 2 programs;
    - (ii) Ensure that resources are managed effectively to care for patients; or
    - (iii) Determine the need for adjustments to payment policies to enhance care or coverage for patients with SUD.
  - (2) Review of appropriateness of medical care, medical necessity, and utilization of services.
    - Restrictions on review of patient records
      - ✓ Can review but not copy or remove client records
      - ✓ Copy or remove but must destroy once audit complete
      - ✓ Client identifying info can only be disclosed back to the program
- ❑ Referral programs do not require an authorization to make a referral

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2: 2024 Updates



- **Single Consent**-SUD clients can now complete one disclosure request to release records for purposes of treatment, payment and healthcare operations (TPO).
  - Allows a single consent for all future uses and disclosures for treatment, payment, and health care operations.
  - Allows HIPAA covered entities and business associates that receive records under this consent to redisclose the records in accordance with the HIPAA regulations.
  - Prohibits combining patient consent for use/disclosure of records for civil, criminal, administrative or legislative proceedings with patient consent for any other use/disclosure.
  - Requires each disclosure made with patient consent include copy of consent or a clear explanation of scope of consent.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, 2024 Updates cont'd.



- **Breach Notification**: Applies the same requirements of the HIPAA Breach Notification Rule to breaches of records under Part 2.

- **Patient Notice**: Aligns Part 2 Patient Notice requirements with the requirements of the HIPAA Notice of Privacy Practices.

- **Safe Harbor**: Creates a limit on civil or criminal liability for investigative agencies that act with reasonable diligence to determine whether a provider is subject to Part 2 before making a demand for records in the course of an investigation. The safe harbor requires investigative agencies to take certain steps in the event they discover they received Part 2 records without having first obtained the requisite court order. Further clarifies/strengthens reasonable diligence steps investigative agencies must follow to be eligible for safe harbor status.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, 2024 Updates cont'd.



- **Other Uses and Disclosures:**
  - Permits disclosure of records without patient consent to public health authorities, provided that the records disclosed are de-identified according to the standards established in the HIPAA Privacy Rule.
  - Restricts the use of records and testimony in civil, criminal, administrative, and legislative proceedings against patients, absent patient consent or a court order.

- **Penalties**: Aligns Part 2 penalties with HIPAA by replacing criminal penalties currently in Part 2 with civil and criminal enforcement authorities that also apply to HIPAA violations.

- **Segregation of Part 2 Data:** Added an express statement that segregating and segmenting Part 2 records is not required, when a Part 2 provider or covered entity receives Part 2 records (either written or verbal) as a result of a client authorization/consent.

- **Complaints:** Added a right to file a complaint directly with the Secretary for an alleged violation of Part 2. Patients may also concurrently file complaint with the Part 2 program.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, Restrictions and Requirements



- **42 CFR Part 2 Restrictions and Requirements:**
  - **Qualified Service Organizations (QSO):** Restrictions on use and disclosure in the regulations in this part do not apply to the communications between a part 2 program and a QSO, which has entered into a written agreement and provides services (not including treatment) such as data processing, billing, dosage preparation, laboratory analyses, accounting, population health management, etc. (Comparable to HIPAA Business Associate).
  - **Reports of Child Abuse or Neglect:** The restrictions on use and disclosure in the regulations in this part do not apply to the reporting under state law of incidents of suspected child abuse and neglect to the appropriate state or local authorities. However, the restrictions continue to apply to the original substance use disorder patient records maintained by the part 2 program including their use and disclosure for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect.
  - **Crimes on Part 2 Program Premises or Against Part 2 Program Personnel:** The restrictions on use and disclosure in the regulations in this part do not apply to communications from part 2 program personnel to law enforcement agencies or officials which:(i) Are directly related to a patient's commission of a crime on the premises of the part 2 program or against part 2 program personnel or to a threat to commit such a crime; and (ii) Are limited to the circumstances of the incident, including the patient status of the individual committing or threatening to commit the crime, that individual's name and address, and that individual's last known whereabouts.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, Restrictions and Requirements cont'd.



- **Communication within a Part 2 program or between a Part 2 program and entity having direct administrative control over Part 2 program §2.12(3)**
  - Communications of information between or among personnel having a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment, or referral for treatment of patients with substance use disorders if the communications are:
    - (i) Within a Part 2 program; or
    - (ii) Between a Part 2 program and an entity that has direct administrative control over the program (e.g., SUD contract provider and DBH SUD)
- **Prohibition of Re-disclosure (§ 2.32)**
  - Individuals or entities who receive patient records directly from a Part 2 program or other lawful holder of patient identifying information and who are notified of the prohibition on re-disclosure must obtain patient authorization form consenting to release of specified records unless:
    - Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2.
    - It is a covered entity or business associate and has received the record for treatment, payment, or health care operations, or
    - Has received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E.

# Confidentiality of Substance Use Disorder Records - 42 CFR Part 2, Non-Part 2 Treating Providers

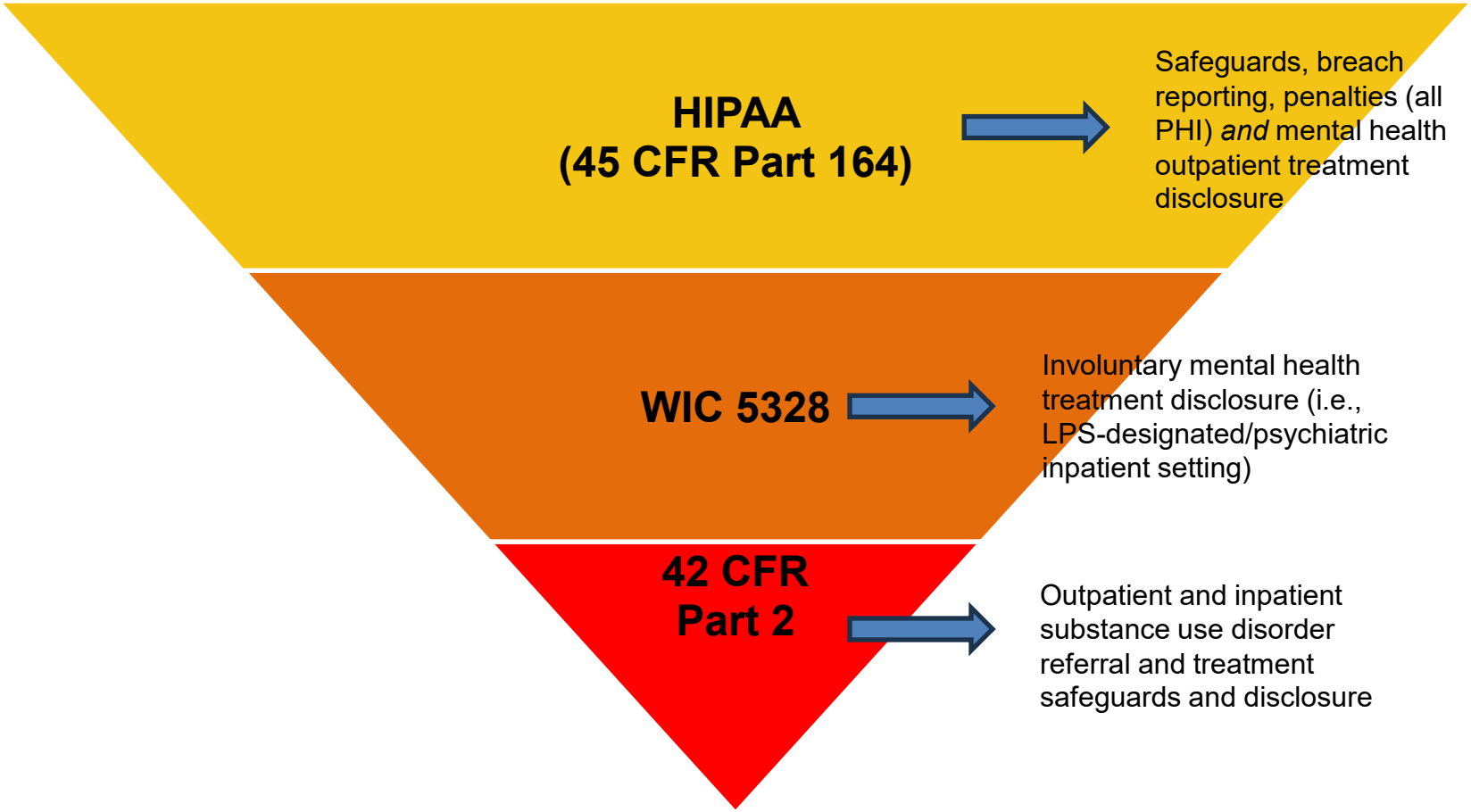


- A non-Part 2 treating provider may record information about a substance use disorder (SUD) and its treatment that identifies a patient. This is permitted and does not constitute a record that has been re-disclosed under Part 2, provided that any SUD records regarding legal notes remain separate and segregated. The act of recording information about a SUD and its treatment does not by itself render a medical record created by a non-Part 2 treating provider as subject to the restrictions of Part 2.

# Privacy Laws Governing Behavioral Health



## Inverted Pyramid – Privacy Laws



# CalAIM Data Sharing Information



LET'S TALK

CalAIM

# CalAIM Data Sharing Information cont'd.



- CalAIM requires the exchange of information about Medi-Cal Enrollees, including an array of administrative, clinical, social, and human service information across sectors.
  - This exchange must occur in adherence with federal and state privacy laws, regulations, and other data sharing rules.

- Guidance provided by Department of Health Care Services (DHCS) supports the CalAIM Data Sharing Agreement, which provides data sharing information between Managed Care Plans, health care providers, community-based social and human service providers, local health jurisdictions, county Mental Health Plans and other public agencies that provide services and manage care under CalAIM.
  - Applicable state and federal law related to mental health and/or SUD PHI must still be applied.

# CalAIM Data Sharing Information, cont'd.



## AB133 – California Health Bill

- Promotes access to behavioral health services for inmate's post-release (exiting jails and youth correctional facilities).
  - Amended Penal Code Section 4011.11 paragraphs (1) through (4) of subdivision (h) and requires that county jail and youth correctional facility inmates be provided assistance in enrolling into health insurance affordability programs, such as Medi-Cal. Paragraph (5) of subdivision (h) is intended to ensure that jail inmates and youth correctional inmates have access to behavioral health treatment in the community post-release.*
- Requires all specified entities to exchange health information or provide access to health information to and from other specified entities in real-time.
- A limited waiver of state law is permitted for purposes of both assisting jail and youth correctional inmates with applying for health insurance affordability programs (which may include applying for those programs while incarcerated or after release) and ensuring those inmates have access to behavioral health services post-release.

***Note:** These two goals are interconnected, since obtaining health insurance is often critical to obtaining continued access to behavioral health services.

## AB2526 – Incarcerated Persons: Health Records

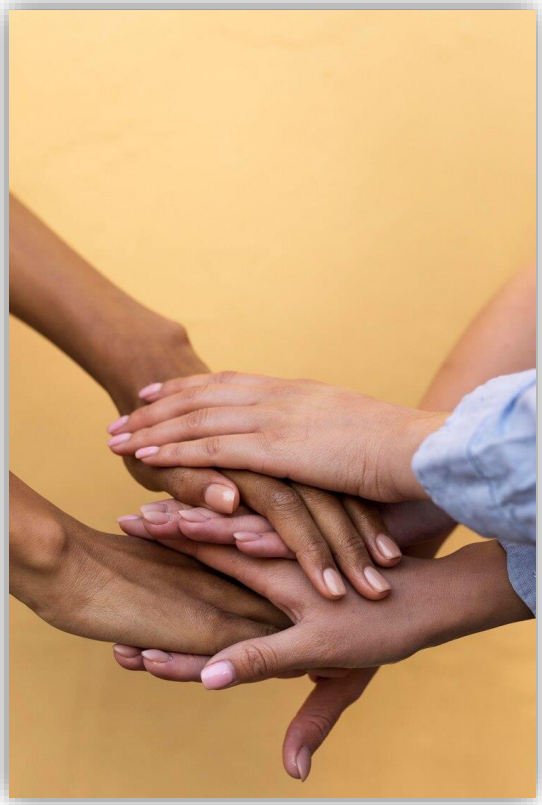
- Applies when an inmate (within the jurisdiction) is transferred from or between the Department of Corrections and Rehabilitation, the Department of State Hospitals, or county agencies caring for inmates, facility may electronically disclose mental health records for an inmate who received services while in custody of the transferring facility.
  - Amended Civil Code 56.10 requiring the electronic transmission of health records for an inmate to ensure sufficient mental health history is available for satisfying specified requirements relating to parole and to ensure the continuity of mental health treatment of an inmate being transferred between those facilities.
  - In addition, Civil Code 56.10 requires all transmissions made pursuant to these provisions comply with specified provisions of state and federal law, including the Confidentiality of Medical Information Act.

# CalAIM Data Sharing Information cont'd



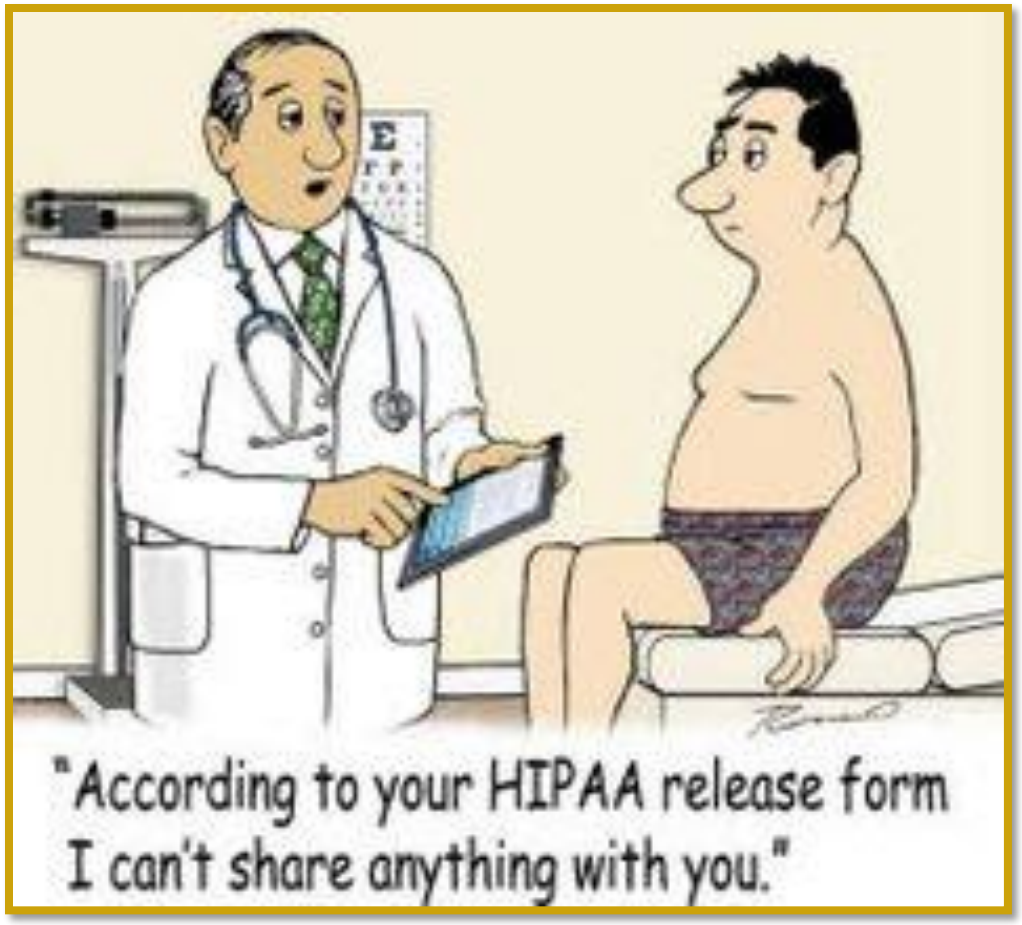
**AB1948 –** Homeless Multidisciplinary Team

- Establishes a homeless adult and family multidisciplinary personnel team with the goal of facilitating the expedited identification, assessment, and linkage of homeless individuals to housing and supportive services.
  - Data sharing for homeless individuals allows provider agencies the ability to share confidential information for the purpose of coordinating housing and supportive services to ensure continuity of care.
  - Data sharing will apply until the identifying individual at risk of homelessness affirmatively opts out of having their information shared.
  - Existing federal or state privacy laws regarding confidentiality and privacy will be adhered to, ensuring information or writings disclosed, exchanged, or acquired are protected (WIC §18999.81).



# Access and Authorizations






Source: Google Images

# Access to Records



- Per HIPAA, a client must have access to their own medical record in any form requested.
- Client's request to inspect medical records must be allowed to occur within 5 working days of written request.
- Client shall receive copy within **15 working days** after written request for record (unless more time is needed and justified).
  - If an extension is needed the requestor must be notified and delivery must not exceed **30 days** from the initial written request date.

***Note:*** DBH retains the records of DBH contract agencies that are no longer in business or no longer have contracts with DBH.

# Authorization to Release PHI



Authorization to Release PHI Requirements:

- Must follow state and/or federal laws (whichever is most stringent) when disclosing client information.
- An authorization must be obtained to disclose PHI unless there is an exception allowing disclosure without an authorization.
- When in doubt, it is best practice to consult a supervisor, a Compliance professional, or move forward with obtaining an authorization.
- Information cannot be provided to anyone other than the client unless there is an authorization or exception that permits the disclosure.
  - It is important to consider which privacy law is governing the PHI (mental health or SUD), and if an exception to requiring an authorization exists (as discussed in this presentation).

# Minor Consent and Authorization



**AB 665 – Minor's Consent to Mental Health Treatment:**

- Authorizes a minor who is 12 years of age or older to consent to mental health treatment if the minor is mature enough to participate intelligently in the outpatient services or counseling services.
- Minors do not need to be an alleged victim of incest, child abuse, nor need to be a present danger of serious physical harm to themselves or others to be eligible for consenting to services.

**AB 816 – Minor's Consent to Medical Services:**

- Authorizes a minor who is 12 years or older to consent to medical and counseling services relating to a diagnosis/treatment of a drug/alcohol problem. This bill also authorizes a minor who is 16 years of age or older to consent to replacement narcotic abuse treatment to opioid use disorder medications from a licensed narcotic treatment.

**Minor Consent to Obtain, Access, or Release PHI:**

- A minor client between the ages of 12 and 17, authorized to consent to medical treatment, is legally entitled to inspect or obtain copies of their medical record.
- Prior to medical records release, it is the responsibility of the health care provider to ensure disclosure of sensitive PHI is **not** detrimental to the minor client.
- In addition, existing federal or state privacy laws regarding confidentiality and privacy will be adhered to ensuring information or writings disclosed, exchanged, or acquired are protected (HSC 123110).
- The provider can only share the minor's medical records with parents if there is a signed authorization from the minor.

# Privacy and Security Incidents versus Actual Breaches



# Privacy or Security Incidents



- Not all incidents are breaches most are policy violations, such as, but not limited to, the following:
  - Sending an email containing PHI outside of entity network to the correct recipient but unencrypted;
  - Sending email, fax or initiating phone call disclosing PHI to incorrect DBH employee, or
  - Leaving encrypted password protected laptop and other mobile devices unattended, resulting in theft.
- There are a number of determining factors for identifying a breach including:
  - Whether the acquisition, access or use resulted in further disclosure;
  - Whether the recipient was authorized to access the PHI, and
  - Whether the PHI was able to be accessed and/or retained by an unauthorized recipient.
- **All** incidents involving inappropriate disclosure of PHI must be reported to the Office of Compliance immediately upon discovery for breach determination.

# Privacy or Security Breaches



Examples of breaches:

- Giving appointment card, discharge summary, letter, etc., to incorrect client without immediate retrieval;
- Giving prescription to incorrect client without immediate retrieval;
- Being unable to locate a medical record or chart note after an exhaustive search is conducted;
- Having an unencrypted laptop or mobile device and leaving it unattended, resulting in theft;
- Sharing client PHI without an authorization not covered by an exception.

# Privacy or Security Incidents




Source: Google Images

# Compromise of PHI



When Client PHI is inappropriately disclosed it must be reported to the Office of Compliance immediately upon discovery:

- Incidents are evaluated by Compliance to determine risk of compromise to client PHI.
- If determined to be a breach, Compliance will proceed with the following:
  - Client notification regarding breach including identifiers disclosed, mitigation completed, contact information, credit monitoring services etc.
  - Department of Health Care Services notification
  - Department of Health and Human Services notification

# Safeguarding PHI



In order to avoid policy violations and breaches there are a number of basic safeguards that must be employed (this list is not exhaustive):

- Ensure PHI is provided to the correct client by conducting visual verification of document and client identification;
- Return or scan all paper documents containing PHI to the client record, log record in/out of chartroom as applicable;
- Ensure laptops, mobile devices, USB drives are password protected and paper documents containing PHI are in a locked case and never left unattended;
- Encrypt all emails containing PHI that are sent outside of the secured DBH or Agency network, and
- Do not include any client identifiers on the subject line of emails.

***Note***: Client identifiers include subsets of the HIPAA List of 18 identifiers (i.e. client initials).

# Questions



# Contact Information



## DBH Office of Compliance

General Questions:
909-388-0879
DBH-ComplianceQuestions@dbh.sbcounty.gov

Reporting Privacy Incident or Breach:

dbh-privacyincidents@dbh.sbcounty.gov