

Challenges of HIE for Medicaid Agencies

Presented By:

Roberta M. Ward

Privacy Officer and Senior Counsel

Department of Health Care Services

Sacramento, California

www.dhcs.ca.gov/privacyoffice

MMIS Conference

August 15, 2007



Legal Limitations on Medicaid Data Disclosures



HIPAA Overview

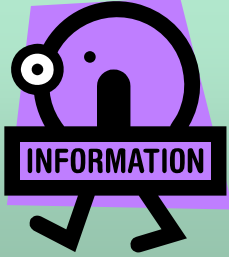
- In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA)
- Title II – Administrative Simplification
 - Transaction standards
 - Security standards
 - Unique identifiers
 - Privacy standards
- Who is covered?
 - Providers
 - Health Plans, such as Medicaid
 - Clearinghouses



The General Privacy Rule

- “Covered entities” may ***not*** use or disclose “Protected Health Information” (PHI)
 - Except as permitted or required by the Privacy Rule
 - Except as authorized by the individual





What is PHI?

- **PHI** is information that identifies or can be used to identify an individual
- Information that relates to the:
 - Past, present or future health condition of that individual
 - Health care provided to that individual
 - Payment for that health care
- Information in any form, including paper, electronic (**ePHI**), and oral communications

What Constitutes PHI – 18 Identifiers

- Name
- Address – Street address, city, county, zip code (more than 3 digits) or other geographic codes
- Dates directly related to patient (except year), including DOB, admission or discharge date
- Telephone & FAX Numbers
- Driver's License Number
- Email Addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License number
- Any vehicle or device serial number, including license plates
- Web Addresses (URLs)
- Internet Protocol (IP) Address
- Finger or Voice Prints
- Photographic Images
- Any other unique identifying number, characteristic, or code
- Age greater than 89 (as the 90 year old and over population is relatively small)

Types of Use & Disclosure

- **Permitted uses & disclosures** are uses and disclosures that are allowed by HIPAA
 - Treatment
 - Payment
 - Health Care Operations
 - Health Oversight
 - Public Health
- **Required disclosures** are mandated disclosures by HIPAA

NOTE: Stricter state or federal laws for a specific program regarding use and disclosure must be followed.

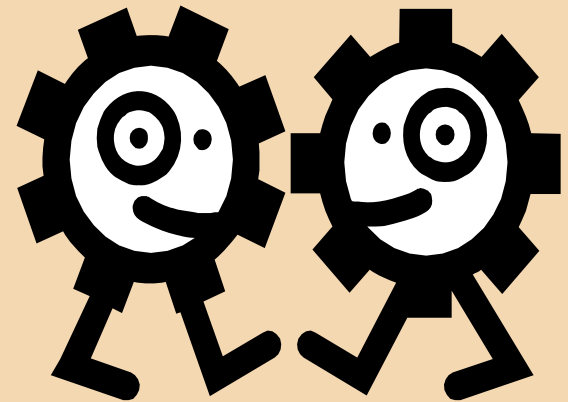
You May Use or Disclose PHI For TREATMENT



- **Treatment** is providing health care to an individual by a health care provider or coordination or management of health care by a health care provider with a third party or referral for care by health care providers
- Treatment only applies to health care providers
- Treatment is not provided by health plans, such as Medicaid, but plans may disclose PHI about an individual to a health care provider for that provider's treatment of the individual. See 45 CFR §164.506.

You May Use or Disclose PHI For HEALTH CARE OPERATIONS

- **Health Care Operations** (HCO) are those activities that support treatment and payment. For example:
 - prior authorizations
 - internal auditing
 - management reviews
 - administrative appeals
- Minimum necessary applies





What is Minimum Necessary?

- Limit PHI access to the smallest amount necessary to do the job
- Use, request, and disclose the minimum amount of information necessary

**HIPAA limits most uses and disclosures of PHI to the minimum amount needed*



Health Plans & Providers May Share PHI For HCO

42 CFR §164.506(c)

- **Each** covered entity must have or have had a relationship with the patient **and**
 - Disclosure is for one of the following:
 - Fraud & abuse detection or compliance
 - Quality assurance, case management and care coordination
 - Reviewing qualifications or competence of health care professionals, health plan performance
 - Training
 - Accreditation, certification, licensing or credentialing activities



PreEmption

(45 CFR Subpart B)

- HIPAA Privacy Rule is a national floor of privacy protection, it does not preempt the field in medical privacy
- If there is a state or federal statute or regulation which:
 - 1) Affords greater protection to an individual's privacy **OR**
 - 2) Provides a greater right to the individual to access their own records

THEN that law prevails over HIPAA
- Sometimes it is possible to read HIPAA Privacy Rule & state law together
- State law must be contrary to the HIPAA Privacy Rule and less stringent in order to be preempted by HIPAA



Federal Preemption

- Federal Preemption is when another federal statute or regulation is contrary to, and more stringent than, the provisions of the Privacy Rule.
- If the federal statute or regulation relating to the privacy of PHI is more stringent, in comparison to a standard, requirement or implementation specification of the HIPAA Privacy Rule, the provision of the federal law controls.

More Stringent Means

- With respect to a use or disclosure, the federal law prohibits or restricts a use or disclosure in circumstances where the use or disclosure would be permitted under HIPAA.
- Except to the Secretary for determining compliance, or
- To the individual who is the subject of the PHI, or
- Permits greater rights of access or amendment to the individual who is the subject of the PHI.

What does this mean for the Medicaid program?

- Medicaid rules on use and disclosure are much more restrictive than HIPAA.
- The federal Medicaid statute and regulations restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the state Medicaid program (section 1902(a)(7) of the Social Security Act and 42 CFR 431.300 et seq).
- States are required to have statutes that provide legal safeguards against uses or disclosures of Medicaid information for purposes not directly connected with the administration of Medicaid and which impose sanctions for violations.

Purposes directly connected with Medicaid Administration are narrowly defined as:

- Establishing eligibility, determining the amount of medical assistance, providing services for recipients and conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to Medicaid program administration.



Medicaid agencies must safeguard information about applicants and recipients, including:

Names and addresses; medical services provided; social and economic conditions or circumstances; agency evaluation of personal information; medical data including diagnosis and past history of disease or disability; any information received for verifying income eligibility and amount of medical assistance; any third party liability information.

Medicaid agencies must inform the court of the restrictions on use and disclosures in response to a subpoena for a case record or for an agency representative to testify concerning an applicant or recipient.



How do Medicaid restrictions on use and disclosure intersect with the HIPAA Privacy Rule?

- **HIPAA permissible disclosures are generally not allowed under Medicaid:**
- **The Medicaid agency may not disclose PHI to:**
 - Public health authorities
 - Researchers, unless research is related to operation of the Medicaid program
 - In response to a subpoena, unless subpoena is for criminal or civil cases related to the Medicaid program, such as fraud and abuse
 - Coroners, medical examiners and funeral directors
 - Law enforcement, unless Medicaid fraud investigation or prosecution
 - Public safety or security reasons
 - In response to a court order, without informing the court first of the restrictive Medicaid rules on use and disclosures

What about the right of Medicaid beneficiaries to access their own records?

- Prior to HIPAA, information could only be released to beneficiaries for purposes directly connected with Medicaid operations.
- Post HIPAA, contrary laws may not restrict health plan beneficiaries' rights to access or amend their own records.



Medicaid and HIE



Use of Medicaid Data for HIE

- Medicaid client information may only be shared by Medicaid agencies:
 1. For purposes directly connected with operation of the Medicaid program, such as providing services to Medicaid beneficiaries.
 2. With Medicaid health plans for case management and care coordination, for example, so long as: the Medicaid health plan has or has had a relationship with the Medicaid patient.
 3. With treating health care providers, so long as the provider is currently treating the Medicaid patient and the relationship is validated.

Release of Information

42 CFR §431.306

- (a) The Medicaid agency must have criteria specifying the conditions for release and use of information about applicants and recipients.
 - (b) Access to information concerning applicants or recipients must be restricted to persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the agency.
 - (c) The agency must not publish names of applicants or recipients.
-
- (e) The agency's policies must apply to all requests for information from outside sources, including governmental bodies, the courts, or law enforcement officials.”

Overview of the CalMEND Performance Improvement Project (PIP):

Reducing Use of Antipsychotics and Polypharmacy in Providing Treatment to Medicaid Patients with Serious Mental Illness

- Medi-Cal statistics reflect that the use of antipsychotics increased 63% from 1994 through 2004.
- Nationally individuals with serious mental illness die on average 25 years earlier than general population with greater morbidity of preventable conditions such as diabetes, metabolic disorders and cardiovascular diseases.
- DHCS and seven county mental health plans formed PIP work group to investigate scope of problem.
- Each county signed confidentiality and data sharing agreement.



Overview of the CalMEND Performance Improvement Project (PIP)

- DHCS provided each county mental health authority with claims/utilization data for Medi-Cal benes served within the county. First dataset based upon 2006 six months claims history.
- Quarterly releases have been scheduled to enable longitudinal analyses and assessments to reduce inappropriate polypharmacy.
- Reports can identify clients who receive a high number of psychotropic medications. Individual providers will be contacted for clinical consultations and recommendations.
- Data sharing will help ensure that clients receive care that is safe, effective and will serve to improve communication, coordination and increase patient safety.



E-Prescribing

- DHCS intends to launch project for purpose of improving quality and reducing medication errors through the exchange of standardized clinical information between Medi-Cal and its providers.
- The pilot will bring medication histories to the point of care in selected communities.
- The exchange of standardized clinical information between the Medi-Cal program and its providers should result in a reduction in medical errors and therefore, improvement in quality of care.

Security Concerns





Identity Theft

- Identity theft occurs when someone uses your personally identifying information, like your name, SSN, or credit card number, without your permission, to commit fraud or other crimes.
 - Different types of identity theft:
 - Financial identity theft
 - Posing as someone else to obtain medical care
 - Prescription fraud
 - Billing fraud
 - Theft of physician identity

Incidence



- The FTC's consumer complaint database shows 670,000 consumer complaints in 2006 – 36% of these related to identity theft or 246,035 complaints.
 - http://www.consumer.gov/sentinel/Sentinel_CY_2006/executive%20summary.pdf
- These are only reported consumer complaint numbers – the FTC estimates that as many as **9 million** Americans have their identities stolen each year.
 - <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>



Financial Identity Theft Using Health Records

- A Rhode Island woman was found guilty of six counts of fraud after it was learned that she preyed on four cancer patients while working as a registration clerk at the Dana-Farber Cancer Institute at a Boston Hospital. She obtained the job by working for a temp agency. She not only committed fraud by accessing patient financial information, but she also defrauded co-workers at another location of approximately \$4,000.



Medical Identity Theft

- Medical identity theft occurs when someone:
 - Uses a person's name and sometimes other parts of their identity (such as insurance information) without the person's knowledge or consent to obtain medical services or goods.
 - Uses the person's identity information to make false claims for medical services or goods.

Posing As Someone Else to Obtain Medical Care



- A Pennsylvania man discovered an imposter had used his identity at 5 different hospitals to receive approximately \$144,000 worth of treatment. At each hospital, the imposter created medical histories in the victim's name.
- *United States v. Sullivan*, Affidavit of Probable Cause for Arrest Warrant, cited in: AG Corbett announces arrest of Philadelphia man in \$144,000 identity theft scam, Attorney General Press Release, July 29, 2005, reported in World Privacy Forum, *supra*, at 7.

Billing Fraud



- In southern California, Medicare patients were given medical tests by non-physicians and had false diagnoses inserted into their medical files by an organized network of medical imaging companies.
- The victims were actively recruited with the promise of free transportation, food, and medical care.
- Once the criminals obtained their personal information and Medicare cards, they used the information to make false claims for more than \$900,000.
- Elizabeth S. Roop, *Stealing You – Medical Identity Theft*, Radiology Today, 7(21), at 16.

Theft of Physician Identity



- A Tennessee doctor's Medicare provider number was illegally obtained by a couple, who proceeded to bill false claims in his name, obtaining more than \$1 million in payments from Cigna Medicare.
- Elizabeth S. Roop, *Stealing You – Medical Identity Theft*, *Radiology Today*, 7(21), at 16.



What is a Breach?

- A “breach of the security of the system”:
 - Is the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”

AND

- Must be disclosed to any resident of the state whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person.



California Breach Notification Statute

- **SB 1386 (Peace, Chapter 915, Statutes of 2002)** effective July 2003, requires a state agency, or any person or business that owns or licenses computerized data that includes personal information, to disclose any breach of security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- The law is codified at Civil Code section 1798.29 and 1798.82. A bill currently pending in the California Legislature, AB 1298, will expand data that triggers breach notification to include medical information and health insurance policy information.

Summary of Privacy Breaches Reported to the Medi-Cal program (between April 2005 and August 2006)

- 18 breaches were reported to the Medi-Cal program by one health plan partner between 4/2005 and 8/2006
 - 7 stolen/lost laptops
 - 3 website incidents – unsecured
 - 3 misdirected mailings
 - 2 incidents of unauthorized use
 - 1 flash drive lost
 - 1 briefcase stolen
 - 1 incident of paper records stolen

Note: all of the reported incidents involved PHI. Some required breach notification as they were unencrypted electronic disclosures involving member names and SSNs



Breach Notifications and Sanctions

- Medicaid agencies must send notices to beneficiaries impacted by data breaches under state laws.
- Medicaid agencies must notify CMS of data breaches involving Medicaid program, as well as notifying other state law enforcement and control agencies.
- CMS sent out state Medicaid director letter warning Medicaid agencies of potential fiscal sanctions and loss of Federal Financial Participation (FFP) for failure to prevent security breaches.
- There is risk of civil law suits for failure to protect security of PHI.

DHCS Privacy Officer

Roberta Ward

Privacy Officer

Office of Legal Services

Phone: (916) 440-7750

Email: PrivacyOfficer@dhcs.ca.gov

Website: www.dhcs.ca.gov/privacyoffice



The End

