Implementing Privacy in a Large Hybrid Entity

Presented by:

Roberta M. Ward, California Department of Health Services, Senior Counsel, Privacy Officer

Susan Fanelli, California Department of Health Services, Privacy Project Manager

Overview

- Centralized Department Effort
- Phased in Approach
- 4 Months to Compliance
- Concentrating First on Covered Functions

Phase 1

Focus on Covered Entities

- Determination of DHS as a Hybrid Entity
- Covered Entity Status Determinations
- Liaisons set up with all DHS covered function areas
- Creation of the Notice of Privacy Practices for each of the 12 health plans and the one provider
- Translation Issues
- First distribution of NPP to all health plan enrollees
- Ongoing distribution of NPPs—stakeholders involved

Department of Health Services (DHS) is a "hybrid entity" under HIPAA

- Hybrid entity is a single legal entity which contains both covered and non-covered functions
- Hybrid must ensure that covered health care components of the entity comply with HIPAA, and
- Do not disclose PHI to another component of the covered entity when the Privacy Rule would prohibit disclosure if the health care component and other component were separate and distinct legal entities

Rules for Hybrid Entities

- Employees of hybrid entity must not use or disclose PHI created or received in the course of work for the covered health care component in a way prohibited by Privacy Rule when they work for both covered and noncovered components of the hybrid.

- Hybrid must document designations of covered health care components and must include any component that would meet the definition of a covered entity if it were a separate legal entity.

إذا أردت الحصول على معلومات عن حقوقك في الحفاظ على السرية الشخصية في نظام الرعاية الصحية لولاية كاليفورنيا (ميدي–كال Medi-Cal) ، اتصل مع رقم الهاتف 255-5259 (916) (Arabic)

Եթե դուք ցանկանում եք տեղեկություն ստանալ ձեր Medi-Cal-ի Գաղտնիության Իրավունքների մասին, ապա խնդրում ենք զանգահարել (916) 255-5259 հեռախոսահամարով: (Armenian)

ប្រសិនបើលោកអ្នកចង់ជ្រាបពត៌មានស្តីអំពីសិទ្ធិឲ្យរអ្វីដែលអ្នកត្រូវទទួលបាន ពី Medi-Cal របស់អ្នក សូមទូរស័ព្ទទៅលេខ (916) 255-5259. (Cambodian/Khmer)

如果你想要得到有關 Medi-Cal 保護個人隱私權利的資料，請致電 (916) 255-5259 (Cantonese)

اگر در مورد محرمانه بودن حقوق Medi-Cal خود اطلاعات میخواهید, لطفا با شماره 255-5259 (916) تماس بگیرید. (Farsi)

Yog hais tias koj xav paub ntxiv txog Medi-Cal Txoj Cai Ceev Tseg, thov hu xov tooj rau (916) 255-5259. (Hmong)

귀하의 Medi-Cal 비공개 권리에 관한 정보를 원하시면 (916) 255-5259로 전화하십시오 (Korean)

如果你希望得到有关 Medi-Cal 保护个人隐私权利的资料，请致电 (916) 255-5259 (Mandarin)

Если Вы хотите получить информацию о том, как в рамках программы Medi-Cal обеспечиваются ваши права на неприкосновенность частной жизни, звоните по телефону (916) 255-5259. (Russian)

Kung nais ninyo ng impormasyon tungkol sa inyong mga Karapatan sa Kalihiman sa Medi-Cal, mangyaring tumawag sa (916) 255-5259. (Tagalog)

Nếu muốn biết thêm thông tin về Quyền Riêng Tư của Medi-Cal, xin gọi số (916) 255-5259. (Vietnamese)

Large Business Associates

- Medi-Cal Fiscal Intermediaries
- Set up process with Contract Management Unit

Training

- HIPAA 101 to all Staff (More than 6100 employees)
- Intranet Based Training deployed through email link
- Able to train 80% of staff within 6 weeks
- Training of Fiscal Intermediaries

Technical Aspects of Training

- Developed in PowerPoint which is equipped to save as html pages
- Emailed link to training on Intranet site
- Linked to quiz to reinforce major points
- Used UserIDs linked to an employee database to verify that training was taken
- Signed Acknowledgment stored by the Supervisors
- Monthly reminders sent to those not trained and new employees

Training Goals

- What functions are covered
- Responsibilities of covered functions
- Responsibilities of non-covered functions
- All employees individually responsible for protection of PHI

Sample Training Slide: DHS Covered Components

- Medi-Cal
- County Medical Services Program (DHS runs program on behalf of counties)
- Children's Treatment Program
- Physicians' Services Contract Back
- Refugee Health Services
- California Children's Services
- Child Health and Disability Prevention Program
- Genetically Handicapped Persons Program
- Medical Therapy Program
- Family PACT
- Newborn & Prenatal Screening
- Aids Drug Assistance Program
- Aids Medi-Cal Waiver
- HIV Diagnostic Assay Program
- Cancer Detection—Prostate Cancer
- Breast and Cervical Cancer Detection Program
- Long Term Care – SCAN
- Long Term Care – PACE

Sample Quiz Question

1. Which of the following is not Protected Health Information?

   A. Billing or medical records maintained by California Children's Services.
   B. Information held by the California Cancer Registry.
   C. Medi-Cal TARS, claim detail reports, prior authorization information, eligibility records.
   D. Records maintained by the Genetic Disease Program that are more than 6 years old.

B is the correct answer, all of the types of information listed except for information held by public health or health oversight agencies are considered to be PHI. Health information within public health or health oversight agencies is protected under other state law.

State of California—Health and Human Services Agency

Department of Health Services

DIANA M. BONTÁ, R.N., Dr. P.H.
Director

GRAY DAVIS
Governor

HIPAA PRIVACY TRAINING ACKNOWLEDGEMENT

I have completed the Department of Health Services HIPAA Privacy Training.

I understand that failure to comply with the Department's privacy policies and procedures is a basis for disciplinary action, including dismissal.

Employee name (please print):	
Division:	**Telephone Number:**
_____ **Employee's signature**	**Date:**

Please give the signed form to your supervisor who will place this in your personnel file.

Development of Department-Wide Policies and Forms

- Creation of Department-Wide Policies/Guidances
- Look at existing state statutes on privacy, access to records, etc.—Information Security Policy, Information Practices Act, Health Administrative Manual
- Forms for exercising rights, Forms Management, Translations
- Sample/Template Letters for Various Responses

Sample Policy: Access

- Need for centralization of access
- Who would be responsible for granting access?
- Development of form for access
  - Verification of Identity
  - Verification of Address
- How to deal with personal representatives
- What to do with Subpoenas

DHS Form 6236

STATE OF CALIFORNIA-HEALTH AND HUMAN SERVICES AGENCY

DEPARTMENT OF HEALTH SERVICES
OFFICE OF HIPAA COMPLIANCE

REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

File Number:_____

You have the right to request to inspect your protected health information in records, which Medi-Cal creates or maintains. You also have the right to request copies of those records. You will be charged for the cost of copying and postage, fees are indicated below. You will receive a response to your request within 30 days after we receive your request and payment. If you want copies of your records mailed, you need to send us a photocopy of your California driver's license, Department of Motor Vehicles Identification Card, or other valid identification. You will also need to send documentation verifying your address. Checks should be made payable to the Department of Health Services (DHS). Mail this completed form to:

Department of Health Services
EDS Communications
P. O. Box 526018
Sacramento, CA 95852-6018
(916) 636-1980

INDIVIDUAL INFORMATION			
LAST NAME		FIRST NAME	MIDDLE INITIAL
ADDRESS		CITY/STATE	ZIP CODE
BENEFICIARY ID NUMBER		DATE OF BIRTH	
DAYTIME TELEPHONE NUMBER ( )	EVENING TELEPHONE NUMBER ( )	EMAIL ADDRESS	BEST HOURS TO REACH YOU

PROTECTED HEALTH INFORMATION YOU WANT TO ACCESS

WHAT TYPE OF PROTECTED HEALTH INFORMATION DO YOU WANT TO ACCESS?

☐ CLAIM DETAIL REPORTS, which show claims paid by Medi-Cal for services received. **($25 fee)**

☐ TREATMENT AUTHORIZATION REQUEST SCREENS. Printouts show which providers have requested services including the type and quantity, whether services were approved, denied, modified, or deferred, including a simple description of the decision, and whether the provider has billed for these services. **($15 fee)**

☐ CASE MANAGEMENT RECORDS, which show case manager notes. **($15 fee)**

☐ OTHER _____

☐ OTHER _____

STATE OF CALIFORNIA-HEALTH AND HUMAN SERVICES AGENCY

DEPARTMENT OF HEALTH SERVICES
OFFICE OF HIPAA COMPLIANCE

FOR WHAT TIME PERIOD DO YOU WANT INFORMATION?	
FROM DATE	TO DATE

METHOD TO ACCESS YOUR PROTECTED HEALTH INFORMATION

☐ PLEASE MAIL ME A COPY OF THE REQUESTED INFORMATION.

☐ I WISH TO REVIEW THE REQUESTED INFORMATION IN PERSON.

☐ I REQUEST THAT A PERSON OF MY CHOOSING BE ALLOWED TO INSPECT MY RECORDS.

NAME

TELEPHONE NUMBER ( )

ADDRESS

RELATIONSHIP TO YOU

IF YOU REQUEST TO REVIEW RECORDS IN PERSON YOU WILL BE CONTACTED TO SCHEDULE AN APPOINTMENT.

LOCATION AVAILABLE FOR IN PERSON REVIEW **SACRAMENTO ONLY**

IDENTIFYING INFORMATION

☐ COPY OF IDENTIFICATION ATTACHED

TYPE_____ (CA DRIVER'S LICENSE, CA DMV IDENTIFICATION CARD, BIRTH CERTIFICATE, BENEFICIARY IDENTIFICATION CARD, MANAGED CARE CARD, STATE OR FEDERAL EMPLOYEE ID CARD)

NUMBER_____

I DECLARE UNDER PENALTY OF PERJURY THAT THE INFORMATION ON THIS FORM IS TRUE AND CORRECT.

BENEFICIARY SIGNATURE DATE

DHS 6236 (9/03)

Page 2 of 3

(IF NO IDENTIFICATION IS ATTACHED YOUR SIGNATURE MUST BE NOTARIZED.)

NOTARIZED BY _____ ON _____(DATE)

NOTARY PUBLIC NUMBER _____

UNOFFICIAL UNLESS STAMPED BY NOTARY PUBLIC

☐ ADDRESS VERIFICATION ATTACHED

FORM OF ADDRESS VERIFICATION _____ (UTILITY BILL, PHONE BILL, DRIVER'S LICENSE, ETC.)

NOTE: ANY ATTEMPT TO FALSELY GAIN ACCESS TO PROTECTED HEALTH INFORMATION IS SUBJECT TO LEGAL PENALTIES.

Please enclose check or money order for amount indicated for each type of record requested.

Creation of Privacy Phone Tree

- Grant Enrollees of any of the DHS health plans ability to exercise their privacy rights
- Business Associate as well as Office of HIPAA Compliance responsible for responding to these calls
- Issue of taking calls in multiple languages and for multiple programs
- Scripting of Responses to Frequently Asked Questions

Phase 2

Getting Started

- Mapping of PHI flow through covered entities/health plans
- Formal Assessments Written for each program area
- Kick-off meeting on Policies/Guidances
- Responsibility of Individual Programs to Develop Specific Procedures for the implementation of each policy
- Determination of level at which to draft procedures

Customization of Procedures

- 12 health plans and 1 provider
- Medi-Cal/Medicaid has some 22 Divisions to examine, many of which have multiple programs
- Resources, Resources, Resources?
- Multiple Meetings: Value of In-Person Meetings
- Constant Training of New Liaisons

Example of Customization: Safeguards

- Required to include Administrative, Technical, and Physical Safeguards
- Reasonable to the Organization

Administrative Safeguards: Decision Points

- Type of Staff Training
- Role of Staff Members
- How to Monitor Safeguard Implementation
- Type and Timeframe for Periodic Internal Review of Safeguard Procedures

Technical Safeguards

- Password procedures, expiration date, length and type of characters
- Location of Computer Monitors
- Screen Savers Used/Locking Computer when Stepping Away from Office
- Laptop Policy: How Much Data to be Stored on Laptops, maintaining laptop security

Technical Continued

- Encrypt or Not Encrypt : Databases and or Transfer of Data through email or other method across the Internet
- Change business practices rather than deploy encryption software?
- Sparking of Department-Wide Encryption Effort
- Confidentiality Statements on all Emails

Physical Safeguards

All forms of PHI must be protected, Procedures to Include:

- Securing Paper Files
- Who has access to what Information?
- Confidential destruction or shredding of information
- Procedures for verbal exchanges of PHI: where and when?
- Fax procedures
- Opening of Mail/mail delivery

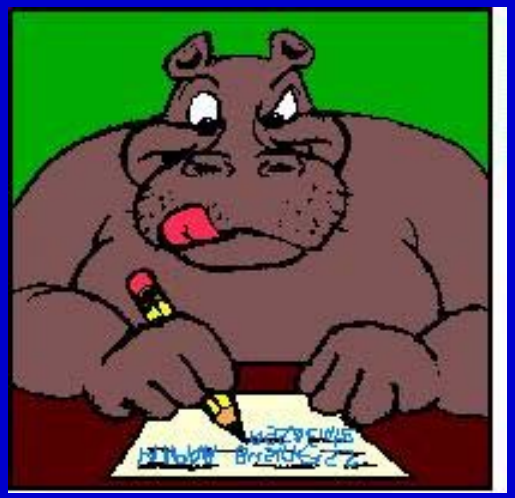
Phase 3: Next Steps

- Ongoing Communication Effort to Protect PHI/Changing Corporate Culture
- Move throughout the hybrid entity to conduct specialized trainings
- Constant Battle for Resources
- Decentralization of Responsibilities of Covered Entities (When?)

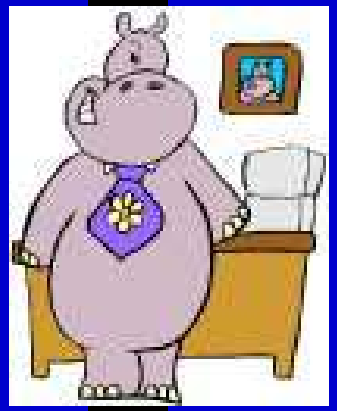
Website Information

- www.dhs.ca.gov/hipaa
- http://www.calohi.ca.gov/state

Dealing with Business Associates



Business Associates



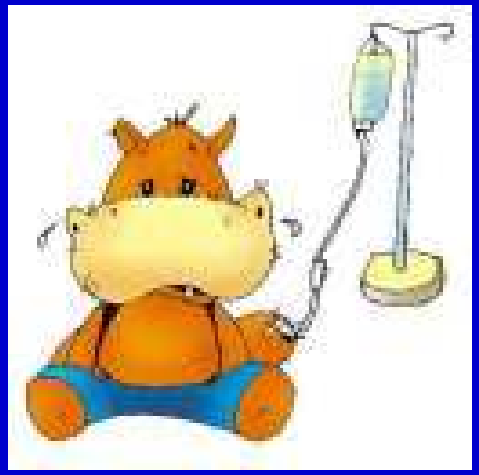
- Business Associates are persons or organizations that, on behalf of a covered entity:
  - Perform any function or activity covered by HIPAA
  - Provide a service on behalf of a covered entity involving the transfer of PHI

Some Business Associates may include:

- A Law Firm
- An Accounting Firm
- A Consulting Company That Provides Data Analysis
- A Third-Party Auditing Agency
- An organization which processes claims

Providers are Not BA's

Treating providers which are paid by the health plan are not thereby business associates of the health plan



Who Are Not Business Associates

- Health Care Providers
  - Trading Partner Agreements may be required
- Entities with which no PHI is exchanged
- Employees of the Hybrid Entity
- Governmental agency authorized by law to determine eligibility for a government health plan

“Internal” Business Associates in a Hybrid Entity

- Internal units outside of the covered programs which perform functions on behalf of the covered programs involving PHI
  - Auditors, Investigators, Attorneys, Accounting, Information Technology

“Internal” Business Associates

- No formal business associate agreements needed
- Need to train “internal” business associates
- “Internal” business associates need to develop policies and procedures for safeguarding PHI
- “Internal” business associates may need to enter into formal Business Associate Agreements on behalf of the covered programs (IT and UR contracts)

Other Covered Entities

- A covered entity may be the business associate of another covered entity
- A covered entity that violates the satisfactory assurances that it will appropriately safeguard PHI as a business associate of another covered entity is not in compliance with the Privacy Rule
(45 CFR 164.502 (e)(1)(iii))

Why Execute a Business Associate Agreement with Another Covered Entity?

- Protects the covered entity contracting-shifts liability for non-compliance to the other entity
- Is required by the Privacy Rule
- Protects the privacy and security of the PHI exchanged
- Allows the covered entity to monitor its contractor's privacy and security policies and procedures

Duty to Monitor

- Outsourcing overseas
- Breaches of security—California Civil Code 1798.29 and 1798.82
- Federal law
- Case law

Under the HIPAA Privacy Rule:

- If Covered Entity knows of pattern of activity or practice of the Business Associate which is a breach of BA's obligations under the BA contract, Covered Entity must take reasonable steps to cure the break or end the violation, or
- If such steps are unsuccessful, terminate the Contractor, or, if not feasible—Report the problem to the Secretary of DHHS.
(45 CFR section 164.504(e)(1)(ii))

Business Associate Template

- On the website of hybrid entity
- May be customized
- Only the Privacy Officer may approve changes

Provisions included in addition to standard provisions of the Privacy Rule:

- Immediate notification of breach
- Employee training and discipline
- Duty to assist in litigation at no cost if responsible

Notification of Breach

- During the term of this Agreement, to notify DHS immediately upon discovery of any breach of security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person. Immediate notification shall be made to the DHS duty officer by pager at 916-328-3605. Written notice shall be provided to the DHS Security Officer and the DHS Privacy Officer within two (2) business days of discovery. Business Associate shall take (i) prompt corrective action to cure any deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations. Business Associate shall investigate such breach and provide a written report of the investigation to the DHS Privacy Officer within thirty (30) working days of the discovery of the breach at the address below:

  Privacy Officer,C/o Office of Legal Services, California Department of Health Services, P.O. Box 942732, MS 0011, Sacramento, CA 94234-7320

Employee Training and Discipline

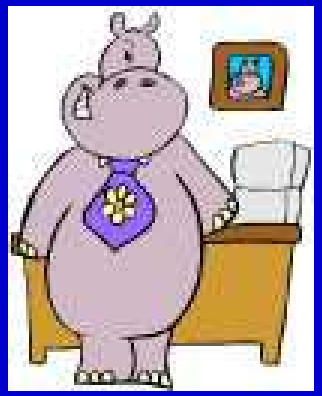
- To train and use reasonable measures to ensure compliance with the requirements of this Addendum by employees who assist in the performance of functions or activities on behalf of DHS under this Agreement and use or disclose PHI; and discipline such employees who intentionally violate any provisions of this Addendum, including by termination of employment.

Assistance in Litigation or Administrative Proceedings

- Business Associate shall make itself, and use its best efforts to make any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHS at no cost to DHS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHS, its directors, officers or employees for claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy based upon actions or inactions of the Business Associate and/or its subcontractor, employee, or agent, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

HMO's

- Many State Medicaid programs have contracted out the operations of Medicaid to private HMO's
- California's Medi-Cal program is about 50/50 fee-for-service and managed care
- Issues: Is the managed care organization (MCO) the business associate of the State Medicaid agency?
- What set of rules apply to uses and disclosures of Medicaid PHI by the MCO?

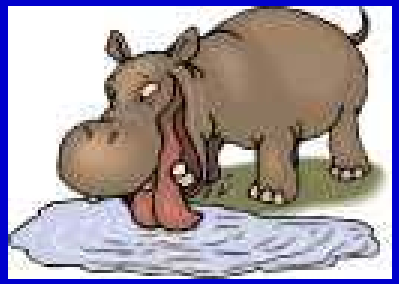


What Are MCO's?

- Could argue that MCO's are business associates of state Medicaid agencies
- Would require business associate agreements
- MCO's would be restricted to same uses and disclosures of PHI as the state Medicaid agency
- Medicaid agency would assume some liability for privacy breaches of MCO's

MCO's Not Medicaid Business Associates

Because MCO's are generally full risk HMO's who are covered entities in their own right and don't like being considered business associates, prevailing view is that they are not business associates of state Medicaid agency.



Contractual Obligations of MCO's

- State Medicaid agency allowed to limit uses and disclosures of PHI under MCO contract to only those restrictive uses and disclosures permitted by federal law for the single state Medicaid agency
- State Medicaid agency can put business associate protections in its contracts with MCO's
- Under the Balanced Budget Act, state Medicaid agency has obligation to ensure HIPAA privacy compliance by its MCO's (42 CFR 438.224)

California MCO Contracts

- Incorporates Business Associate language into MCO contracts
- Limits uses and disclosures to only those permitted for Medicaid state agency and those required by law
- Requires safeguards and a comprehensive written privacy and security program

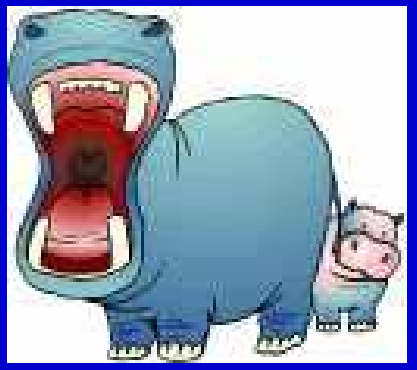
MCO Contracts Continued

- Requires reporting of improper disclosures within 24 hours, investigation, and prompt action to cure breaches
- Requires MCO to include State's Privacy Officer as a contact for complaints
- Requires submission of MCO Notices of Privacy Practices for review

FI Contract Provisions

- **Requires designation of a Privacy and Security Officer**
- Binds the FI to use the State's uniform HIPAA forms
- Requires ongoing HIPAA privacy and security training program

FI Contracts



Other important provisions in fiscal intermediary business associate agreements:

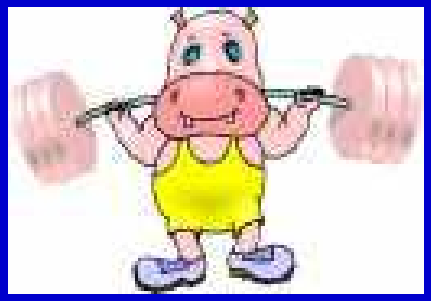
- Written privacy and security policies, duty to assist in defense,
- Time deadlines on duty to provide access to records and amend records,
- Access to internal practices, books and records by covered entity to audit compliance with privacy

Other Governmental Agencies

- Other governmental agencies may work in partnership with the government health program to perform certain functions
- An agency that does not administer a program, but which provides health care services for the program is not a covered entity
- Parts of these other agencies may be a business associate of the governmental health program. 65 Fed. Reg. 82578 (December 28, 2000)
- Business associate language may be incorporated into Memorandums of Understanding, Inter-Agency Agreements, or into regulations.

What to Do If You Can't Get Agreement by April 14, 2004

- Document good faith efforts
- Terminate relationship or cease exchange of PHI
- For governmental business associates required by law to perform a function for the covered entity—may continue to disclose PHI if covered entity documents attempts to get agreement and reason for failure (45 CFR 164.504 (e)(3)(ii))



Balancing Privacy and Need to Know

- Data Matches
- Public Health Registries
  - Cancer
  - Immunization
- Health Oversight—Fraud