

Information Privacy & Security Training

For
Department of Health Care Services
&
Department of Public Health



This Training

The Information Privacy & Security Training is mandatory for all staff in order to:

- Meet legal requirements at the state and federal levels
- Meet requirements of the State Administrative Manual (SAM) & Health Administrative Manual (HAM)
- Train staff on privacy & security laws
- Train staff on protections for confidential information
 - What information is confidential?
 - How do we protect confidential information?

Training Modules

1. The Laws that Protect Confidential Information
2. How We Safeguard Confidential Information
3. Minimum Necessary Use & Disclosure of Confidential Information
4. Uses and Disclosures of Confidential Information
5. Business Associates & Data Releases
6. Access to Patient Records
7. Amendments to Records
8. Accounting of Disclosures
9. Complaints About Use, Disclosure, and Protection of Confidential Information
10. Breaches of Confidential Information
11. Sanctions and Penalties for Violations of Policy and the Law

The Laws that Protect Confidential Information



The Laws that Protect Confidential Information

Federal and State laws require protection of certain types of data that the Department of Health Care Services (DHCS) and Department of Public Health (CDPH) collect and maintain.

- At the Federal level:
 - *Health Insurance Portability and Accountability Act (HIPAA) – Privacy & Security Rules*
- At the State level:
 - *Information Practices Act (IPA)*



HIPAA Overview

Health Insurance Portability and Accountability Act (HIPAA) – Federal law that standardized particular business processes in the health care community including:

- ***Transaction standards*** – Standardized electronic exchanges of data (*Example: Claims transactions*)
- ***Unique identifiers*** – Standardized identifiers used for billing (*Example: Various provider billing numbers standardized to National Provider Identifier*)
- ***Security standards*** – Standardized the protection of electronic data
- ***Privacy standards*** – Standardized the protection of all forms of data

***This training is focused on the HIPAA Privacy & Security Standards

Enforcement of HIPAA

- HIPAA Privacy Rule is enforced by the Office for Civil Rights (OCR) in the U.S. Department of Health & Human Services.

Website: *<http://www.hhs.gov/ocr/hipaa/>*

- HIPAA Security Rule is enforced by U.S. Centers for Medicare & Medicaid Services (CMS)

Website: *<http://www.cms.hhs.gov/>*

HIPAA Applicability

- HIPAA applies to covered entities which include:
 - **Providers** which perform a standard transaction
 - All **Health Plans**
 - Any **Clearinghouse** that performs a transaction on behalf of a provider or health plan
- The Departments of Health Care Services (DHCS) and Public Health (CDPH) contain both provider and health plan functions
- There are programs in CDPH which are not covered by HIPAA, such as Licensing and Certification, Vital Records, Environmental Health, etc...

What Information is Protected by HIPAA?



HIPAA Protects PHI

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



HIPAA Protects PHI Cont...

- HIPAA describes a list of 18 identifiers that constitute PHI.
- If you have any one of these identifiers in your dataset, you have PHI and it must be safeguarded appropriately.
- *For example: A name plus the fact that the person is on Medi-Cal (or CCS or CHDP or IMPACT or EWC) is enough to make information PHI.*

The 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)



What is NOT PHI?

- De-identified data is NOT covered by HIPAA
 - Once you strip the 18 identifiers out of your dataset you have de-identified the data and it is no longer covered by HIPAA.
- HIPAA does NOT cover:
 - Employee Records
 - Workers' Compensation Records
 - Records about Providers
- **HOWEVER**, the Department considers all three of these types of records “personal confidential information” (PCI) which therefore must be safeguarded in the same manner as PHI.



Information Practices Act

(California Civil Code section 1798 et seq.)

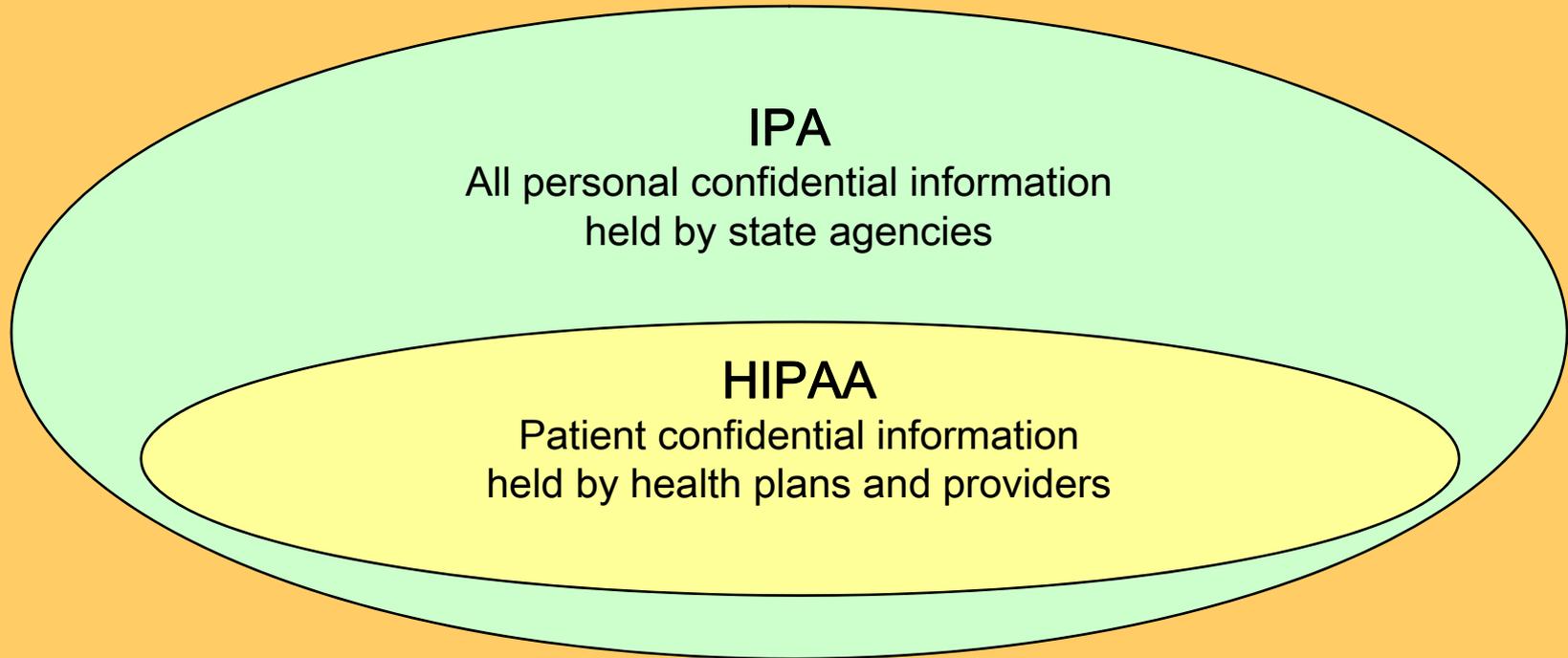
- The IPA (State law) establishes requirements for **all** state agencies for the collection, maintenance and dissemination of personal information.

**What Information is Protected by
the IPA?**

“Personal Confidential Information” (PCI)

- IPA protects **all** personal confidential information (PCI) held by a state agency.
- PCI is information that is not public which identifies or describes an individual including:
 - Names
 - Home Addresses
 - Home Telephone Numbers
 - Social Security Numbers
 - Medical or Employment Histories
 - Personnel Records
 - Licensing Records

HIPAA and the IPA



- The IPA covers a broader amount of information than HIPAA; however, we protect **all** confidential information (PHI and PCI) in exactly the same manner.

Sensitive Information

- ***Sensitive*** information:
 - Is a special kind of information maintained by the Department that requires a higher than normal assurance of accuracy and completeness. .
 - Requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion.
 - May be public or confidential.
- **EXAMPLE:** Department's financial transactions and regulatory actions. This information may not be individually identifiable as PHI and PCI are defined, but this information is sensitive to the Department and must be protected.



Health Administrative Manual (HAM)

- The privacy and security policies for DHCS and CDPH have been codified in the HAM
- HAM Sections 6-1000 through 6-1080 covers Information Privacy and Security Policy
- HAM incorporates the Department's data privacy and security policies and requirements of the SAM (State Administrative Manual)
- HAM is available on the Intranet

How We Safeguard Confidential Information





Safeguards

- We now know the information we need to protect: **PHI**, **PCI**, and **Sensitive Information**.
- We now know the laws and policies that protect PHI, PCI, and Sensitive information: **HIPAA**, **IPA**, and **HAM**.
- Now how do we protect all of the confidential information we collect and maintain?



Types of Safeguards

There are 3 types of Safeguards to protect PHI, PCI, and sensitive information:

– **Administrative**

- Policies and Procedures
- Training

– **Physical**

- Locked buildings and rooms
- Locked desk drawers and cabinets
- Confidential shred

– **Technical**

- Locked computer screens
- Passwords
- Encryption

Administrative Safeguards

Let's start with Administrative Safeguards...

- Our Department's Information Privacy & Security Policy is located in Health Administrative Manual (HAM), Sections 6-1000 through 6-1080. You can get to the policy via the intranet through the Information Security Office webpage or the Privacy Office webpage. You can also use this website:

<http://admin.int.dhs.ca.gov/ham>



Department Requirements

- All Department employees (including State staff, contractors, retired annuitants, student assistants, etc...) are required to read and comply with the HAM. To confirm this, you are required to sign a Security & Confidentiality Statement (**DHS 2420 form**) annually and give this to your supervisor.
- Supervisors are responsible to:
 - Ensure all staff receive training on Department's policy.
 - Maintain a file of signed Security & Confidentiality Statements for all staff that report to them.
 - Monitor staff for policy compliance.
 - Ensure there are written desktop procedures, where necessary.

Policies, Procedures & Training

- This training is considered to fulfill the Department's requirements for Privacy and Security Training
- Management has a responsibility to:
 - Ensure all staff is trained.
 - Create specific desk top procedures.
 - Monitor staff for compliance.

Physical Safeguards

Now let's talk about Physical Safeguards...

- Information/data is one of our Department's most critical resources. State and Federal law, as well as Department policy, requires that the privacy and confidentiality of all personal, confidential (PHI/PCI), and sensitive information be protected. This covers information/data in any form: oral/verbal, paper, and electronic.

The Department implements physical safeguards to protect information and this is how we do it...

Locked Cabinets

- HAM 6-1050.2 states personal, confidential, and sensitive information **MUST** be locked during non-working hours even if the building is secure.
- Put documents in a locked drawer or a filing cabinet.
- Do not leave keys to cabinets and drawers in desk or in any obvious place.
- Do not leave PHI/PCI/Sensitive Information visible on top of or under desks unless your office is locked.



Unattended Areas

- HAM Section 6-1010.1 states to never leave personal confidential or sensitive information unattended, even for a few minutes, including during working hours.
- **Unattended** means that PHI/PCI/Sensitive Information documents are not locked up and are out of sight of management & staff authorized to access the information.
- Another staff member may watch your PHI/PCI/Sensitive information if they are in the immediate area.

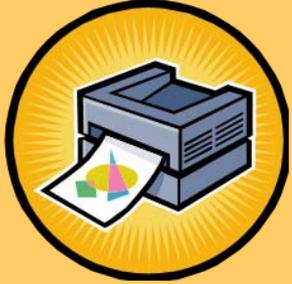




Confidential Destruct

- When you no longer need the PHI/PCI/Sensitive Information for business purposes, you have two options to dispose/destroy this information.
 - You can shred the documents yourself with shredders available in the Department.
 - You can utilize locked, confidential destruct bins. These are large, grey, pad-locked bins that are available in the Department.
- You should not discard PHI/PCI/Sensitive Information at home or away from the Department or in recycle bins or waste baskets.
- Confidential destruct documents are not to be stored in boxes in employees' cubicles or offices (HAM Section 6-1010.1).

Printing, Faxing, & Mailing PHI/PCI



- Printing
 - Do not leave print outs with PHI/PCI/Sensitive Information sitting on the printer.
 - Deliver print outs to appropriate persons immediately or secure in own desk.
- Faxing (HAM Section 6-1050.4)
 - Notify the recipient.
 - **Verify** the fax number.
 - Use a cover page with a confidentiality statement.
 - Do not leave faxes with PHI/PCI/Sensitive Information sitting in the fax machine.
- Mailing (HAM Section 6-1050.5)
 - **Verify** the address.
 - PHI/PCI/Sensitive Information in outgoing correspondence should not be visible.





Safeguards for Mail

- Mail large quantities (reports) of PHI/PCI/Sensitive Information using a secure courier with a tracking system.
- Know what you are sending!
 - Inventory data leaving the Department in case it needs to be recreated.
- Have IT staff encrypt PHI/PCI/Sensitive Information on disks, CDs, and other media before they are mailed.
- Update address directories and databases regularly to ensure PHI/PCI/Sensitive Information is received by the intended recipient.
- See HAM Section 6-1050.5.



Mailing SSNs

(CA Civil Code 1798.85)

- It is *illegal* in California to:
 1. Publicly post or display an individual's SSN.
 2. Print an individual's SSN on any card required to access products or services.
 3. Require an individual to transmit his or her SSN over the internet unless secure connection or encrypted.
 4. Print an individual's SSN on any materials mailed to the individual unless:
 - a) Required by state or federal law.
 - b) In an application or form for enrollment or to establish, amend, or terminate an account or policy (Note: SSN may not be visible on the envelope).

Safeguards for Oral Communications

- Speak quietly when talking about PHI/PCI/Sensitive Information.
- Find enclosed offices to discuss PHI/PCI/Sensitive Information.
- Do not discuss PHI/PCI/Sensitive Information outside of the office with family or friends.
- Do not discuss PHI/PCI/Sensitive Information with those who do not need to know even if they work with you.
- Verify the identity & authority of persons to whom you verbally exchange information (HAM Section 6-1050.7).





Removing PHI/PCI from the Department

- Make sure records are inventoried.
- Lock PHI/PCI/Sensitive Information (paper and electronic) in trunk or where not visible while in route and only while in route.
- Do **not** leave PHI/PCI/Sensitive Information unattended in cars, hotel rooms, luggage, or briefcases.
- Keep PHI/PCI/Sensitive Information in home overnight if necessary.
- Do **not** check PHI/PCI/Sensitive Information in baggage on commercial airplanes.
- Bring all information back to the Department for filing or destruction.
- See HAM Section 6-1050.3.

Technical Safeguards

Now let's talk about Technical Safeguards...

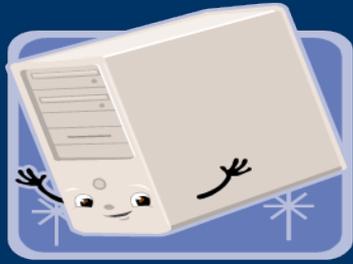
It is the Department's policy to maintain records and equipment using privacy measures that protect privacy and prevent the loss of information through accident, misuse, sabotage or other criminal activity, or natural disaster.

The Department implements Technical Safeguards to protect information/data and this is how we do it...



Passwords

- Select unusual combination of letters, numbers & special characters.
- Change password every 60 days.
- Do **not** share your password.
- Do **not** write your password down.
- Do **not** include your password in a data file, log-on script, or macro.
- Report any suspected unauthorized use of a password to the supervisor and the Information Security Officer (ISO) immediately.



Computing Equipment

- Use Ctrl-Alt-Delete to lock your computer before you leave it unattended.
- Store files on server/shared drives that are backed up. Do not store on desktops.
- Do not use computer equipment for any unauthorized purposes.



Sending PHI via E-Mail

- Always ensure delivery to intended recipient by checking e-mail address.
- Only send the minimum necessary PHI/PCI/Sensitive Information via e-mail.
- Insert a confidentiality statement at the end of your e-mail.
- Do **NOT** send e-mail messages containing PHI/PCI/Sensitive Information **outside** of the Department such as to EDS, DOJ, DSS, or the counties unless you encrypt.

E-Mail Encryption Technology

- ISO has an approved e-mail encryption technology available to all staff.
(<http://itsd.int.dhs.ca.gov/ei/encryption/>)
- It's easy... simply insert “[secure]” in square brackets anywhere on the subject line.
- As soon as you click on “Send” the e-mail is immediately encrypted.
- If the recipient of your e-mail replies, the reply e-mail will automatically be encrypted.



Laptops

- Do **not** leave laptops unattended.
- Do **not** store PHI/PCI/Sensitive Information on a laptop unless it is encrypted.
- Cable lock laptop to an immovable surface.
- When not in use, place laptop in lockable storage.

Mobile Computing Devices



- Examples of devices:
 - Laptops, Tablet PC, PC Notebooks
 - USB storage device
 - PDAs – Palm, Blackberries
 - Flash Memory (memory sticks & cards)
 - Camera phones
- Only download or store minimum amount of PHI/PCI/Sensitive Information on mobile devices.
- Encrypt all mobile devices or data.
- Do **not** download or store SSN's on mobile devices if possible.

Mobile Computing Policy

(HAM Section 6-1020.9)

- Employees agree to take precautions for the mobile device and the information it contains.
- All software installed must be approved by the employee's Branch Chief and the ISO.
- Confidential information should not be downloaded or stored on the device unless absolutely necessary.
- Information that is no longer needed should be disposed of properly.
- If a device is lost, notify the ISO, manager/supervisor and the Privacy Office.

Remember

- Safeguards are only as effective as the people who use them.
- It is up to YOU to make sure that information is kept private and secure.



Minimum Necessary Use & Disclosure of Confidential Information





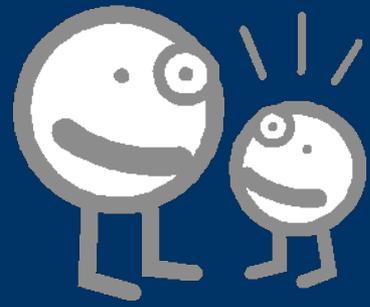
What is Minimum Necessary?

- Minimum necessary is a concept in HIPAA that ensures that PHI is being limited in its use and disclosure and minimizes risk to security of data.
- Access to PHI must be limited to the smallest amount necessary to do your job including:
 - **Using** the minimum amount of information necessary.
 - **Requesting** the minimum amount of information necessary.
 - **Disclosing** the minimum amount of information necessary.



Minimizing Use

- Department staff access should be specific based upon operational need of each unit.
 - Management must limit staff permissions to locked areas with PHI (paper and electronic).
 - Management must work with IT to ensure role-based access to electronic data, meaning staff should only access applications and folders on the server that are applicable to their job.
- Staff must limit forwarding of PHI & printing to relevant fields and records.



Minimizing Request & Disclosure

- Staff should only request to inspect PHI necessary for job function, not the entire record, unless needed.
- Copy only relevant parts of PHI.
- Blackout PHI not relevant to the requested information.
 - Example: SSNs on applications that are copied and placed in files where the SSN is not needed. SSN should be blacked out.



When Minimum Necessary Does **NOT** Apply

- Health care provider for treatment.
 - Doctors can share entire medical charts to care for a patient.
- Individual who is the subject.
 - Patients have the right to access all of their medical record.
- Pursuant to an individual's authorization.
 - A patient can authorize any part or all of their record to be given to another party.
- Disclosures to the Secretary of Health & Human Services.
- When a disclosure is required by law, such as in response to a court order or subpoena

Uses and Disclosures of Confidential Information



Disclosures of Data

(HAM Section 6-1030)

- Managers must ensure that PHI/PCI/Sensitive Information is not released to external entities in violation of federal or state laws or regulations or Department policies.
- Non-routine releases of such data in large quantities must be approved by the Privacy Officer and the Information Security Officer in writing before disclosure.
- See HAM Section 6-1030.



Use & Disclosure

- **Use** is the sharing, application, utilization, examination, or analysis of protected health information within a covered health plan or provider which maintains the information.
- **Disclosure** is the release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

HIPAA

Notice of Privacy Practices (NPP)

- The NPP

- Is required by HIPAA to be mailed to all new health plan enrollees explaining how their information is used and disclosed by a HIPAA health plan.
- Provides contact information for beneficiaries to:
 - Request access or amendment to records.
 - Request an accounting of disclosures.
 - Complain about violations of privacy rights to the Privacy Office or the Office for Civil Rights.

- Web link to NPP's:

<http://www.dhs.ca.gov/privacyoffice/NPP/default.htm>

Types of Use & Disclosure

- **Permitted uses & disclosures** are uses and disclosures that are allowed by HIPAA without the patient's consent or authorization.
 - 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.
- Treatment only applies to health care providers.
- Minimum necessary does **NOT** apply.

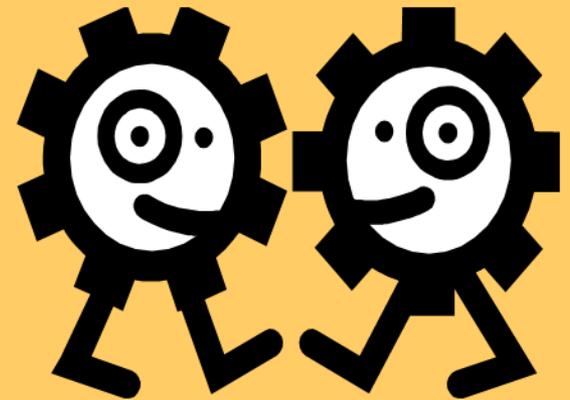
You May Use or Disclose PHI For PAYMENT

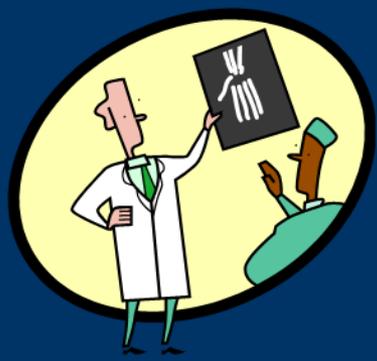
- **Payment** is the compensation for services and include activities to obtain:
 - Premiums if you are a health plan.
 - Money for services if you are a provider.
- Minimum necessary applies.



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.





Health Plans & Providers May Share PHI For HCO

- **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.
 - To provide training to staff.
 - Accreditation, certification, licensing or credentialing activities.

Other HIPAA Permitted Disclosures

- To Health Oversight Agencies
 - That are authorized by law to conduct certain oversight activities.
 - Examples: Department of Justice, Federal Bureau of Investigation, Office of Inspector General, Medical Board, Dental Board.
- To Public Health Authorities
 - That are authorized by law for the purpose of preventing or controlling disease, injury or disability.



Example of Health Oversight

- Covered health plans and providers may disclose PHI to an oversight agency for the purpose of reporting violations of professional standards or problems with quality of care.
- **EXAMPLE:** Medicaid agency may file a complaint with the Medical Board based on PHI received as a result of audits or investigations or routine operations.

What is **NOT** Health Oversight?

- An investigation or activity is **not** considered health oversight if the individual is the subject of the investigation or activity and such investigation does not arise out of and is not directly related to:
 - The receipt of health care.
 - Claim for public benefits related to health.
 - Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services (45 CFR Section 164.512(d)(2)).
- *Example:* Investigation of tax fraud, alimony, domestic violence, etc...
- May report violations of law discovered during health oversight investigation to other agencies for follow-up (e.g. FTB, IRS, DOJ).



Required Disclosures

- Individuals requesting a copy of their own PHI.
- Secretary of the U.S. Department of Health and Human Services.



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 statute or regulation which:
 - 1) Affords greater protection to an individuals' 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.



NO Preemption

(45 CFR 160.203 (c) & (d))

- Public health reporting laws are not preempted (over-ridden) by HIPAA.
- Health plan auditing & licensing & certification of health facilities or individuals are not preempted by HIPAA.
- Medicaid, CHDP & CCS privacy laws and rules are **not** preempted by HIPAA because they are more stringent.



Medi-Cal Program Uses & Disclosures

- California Welfare and Institutions Code section 14100.2 mandates:
 - Medi-Cal program information is confidential
- Medi-Cal uses and disclosures are limited to:
 - The individual regarding his/her own PHI
 - **To purposes directly connected to the administration of the Medi-Cal Program**
- More restrictive use and disclosure than HIPAA!

Examples of Medi-Cal Disclosures

- Purposes directly connected to Medi-Cal administration include:
 - Determining eligibility and reimbursement
 - Providing services to recipients
 - Conducting or assisting investigations, prosecutions or proceedings related to Medi-Cal
 - Third Party Liability activities
 - Audits and legislative investigations
- It is a misdemeanor to disclose Medi-Cal data in violation of this law



Internal Sharing of PHI

- PHI should not be shared with other parts of the Department that do not assist Medi-Cal with its operations
- PHI may be shared with internal Medi-Cal business associates when assisting Medi-Cal operations. Examples are:
 - Legal
 - Accounting
 - Audits and Investigations
 - Children's Medical Services

Child Health & Disability Program

(Health & Safety Code Section 124110)

- CHDP has a very strict statute for disclosure of its data
 - Includes data on CHDP application form and health screening results
 - Need written, informed consent of a parent or guardian of the child or emancipated minor before release of data
 - Research releases, subpoena releases, etc... need specific consent of parent, guardian, or emancipated minor

California Children's Services

(22 CCR Section 41670)

- CCS has a privacy regulation which covers state and local staff administering the program
 - May not divulge personal facts or circumstances without individual consent
 - Exceptions:
 - Necessary to provide services to individual mothers & children (similar to HIPAA treatment, payment, & operations)
 - Data in summary, statistical, or other form which does not identify individuals may be released without consent

Genetically Handicapped Persons Program

- GHPP does not have statute or regulation on privacy of data; however they are covered under 45 CFR Parts 160 & 164 of the HIPAA Privacy Rule and Civil Code Section 1798.24 of the IPA.
- Governed by HIPAA Privacy Rule and State Information Practices Act (IPA).
- IPA has a list of allowable disclosures which should be read in conjunction with HIPAA, but which are either compatible with HIPAA or more liberal than HIPAA, & therefore pre-empted.



Judicial & Administrative Proceedings

(45 CFR 164.512(e))

- Note: When the agency is a plaintiff or defendant in a lawsuit, PHI may be disclosed as part of program operations.
- Regular rules for program operations disclosures apply, such as minimum necessary.



Judicial & Administrative Proceedings, cont...

(45 CFR 164.512(e))

- Permissible Disclosures PHI may be disclosed:
 - In response to an order of a court or administrative tribunal when DHCS is not a party.
 - In response to a subpoena, discovery request, or other lawful process if reasonable efforts have been made to ensure that the individual has been given notice of the request or reasonable efforts have been made to secure a qualified protective order.



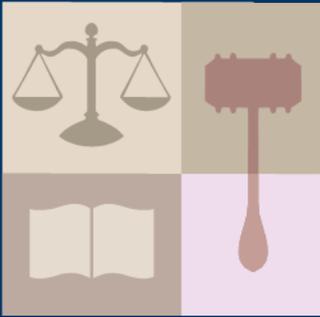
Qualified Protective Order

- An order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
 - Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested.
 - Requires the return to the covered entity or destruction of the PHI at the end of the litigation or proceeding.



Medi-Cal Subpoenas

- The Medi-Cal Program does not usually respond to subpoenas for PHI:
 - Unless it directly relates to the administration of Medi-Cal.
 - Unless it is required by a court order.
- Suggest the individual beneficiary/ personal representative request the PHI through the individual Access Policy.



CMS Subpoenas

- CCS & CHDP require a court order.
- A subpoena may be served by an attorney & does not necessarily have the signature of the judge.
- CCS, CHDP, & GHPP may release information with a signed client/personal representative authorization.
- Use Department authorization form (**DHS 6247**) which is HIPAA compliant & requires that the identity & authority of the requestor be verified.



IPA Releases

(California Civil Code Section 1798.24)

- Under the IPA, a State Agency may release PCI:
 - 1) To the individual to whom record pertains.
 - 2) With prior written voluntary consent.
 - 3) To the guardian or conservator or authorized representative if documented.
 - 4) To a governmental entity when required by law.
 - 5) Pursuant to the Public Records Act.
 - 6) Compelling health or safety.
 - 7) Subpoena or court order if agency attempts to notify individual beforehand.
 - 8) To law enforcement or regulatory agency.

IPA Notice

- The agency must provide a notice on any form used to collect personal information.
- Notice similar to NPP must contain:
 - Name of agency official and authority for maintaining records.
 - Whether submission of information is voluntary or mandatory.
 - Principal purposes for the use of the information.
 - Any disclosures which may be made of the information.
 - Individual's right to access their records.



Releases to Researchers

- Research means a systematic investigation designed to develop or contribute to generalizable knowledge.
- Program evaluation may become research when the contractor intends to publish the results.
- Research proposals involving Department data and/or beneficiaries need to be approved by the Committee for Protection of Human Subjects (CPHS) in the Health & Human Services Agency.

IPA & Disclosure for Research

- Section 1798.24(t) of the Civil Code requires University of California or nonprofit educational institutions to obtain approval from the Committee for the Protection of Human Subjects (CPHS) before any state agency data containing personal information may be released for research purposes.
- CPHS looks at minimum necessary release of data, need for SSNs, & safeguards.





If You Have Any Questions...

- Read the Notice of Privacy Practices for your program.
- Discuss the situation with your manager or supervisor.
- Call your house counsel.
- Contact the DHCS Privacy Officer at (916) 440-7750.

Or

- Contact the CDPH Privacy Officer at (916) 440-7432.

Business Associates & Data Releases





HIPAA Business Associates

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

HIPAA Business Associates Include:

- Medi-Cal Managed Care Plans
- Electronic Data Systems (EDS)
- Delta Dental
- Ramsell
- Maximus
- UCSF, UCLA
- Health Management Systems
- Other State Agencies, such as, Department of General Services, State Controller's Office, Department of Technology Services, etc...





HIPAA & Managed Care Plans

- Medi-Cal Managed Care plans are:
 - Covered entity health plans under HIPAA.
 - Treated as a type of business associate by Medicaid Agency.

State Medicaid Agency Must Ensure Through Contracts:

- That plans use and disclose individually identifiable health information in accordance with privacy requirements in the HIPAA Privacy Rule.

(42 C.F.R. §438.224)



Type of Business Associate Contracts

- There are three versions of business associate contracts:
 - High Risk
 - Standard Risk
 - Managed Care
- To view Business Associate Agreements, please go to the Privacy Office website at:
www.dhs.ca.gov/privacyoffice



Type of Business Associate Contracts, cont...

- High Risk: For fiscal intermediaries & others with large volumes of PHI.
 - Requires Security Officer
 - Compliance with HIPAA Security Rule
 - Compliance with OMB A-130
 - Compliance with specific State security and privacy policies
 - Immediate notification of electronic breaches
- Standard Risk: All other contractors must meet State level of security and privacy protections.
- Exhibit G: A third contract type that was created specifically for managed care.



Data Use Agreements

- For all data disclosures outside of the Department we require either a BAA or a Data Use Agreement (DUA).
- DUAs require:
 - 1) The recipient of the data to use the data for purposes of the agreement only.
 - 2) That the user of the data secure information.
 - 3) The destruction or return of the data when agreement ends.
 - 4) Reporting of breaches.



Confidentiality Provisions of Contracts

- All Department contracts contain a confidentiality section that:
 - Protects the privacy and security of data.
 - Requires the reporting of security breaches.
 - Requires employee training in privacy and security.

Non-Routine Data Releases

ATTENTION ALL DATA RELEASERS!

- All non-routine releases of large volumes of PHI or PCI require prior, written approval of the Privacy Officer and Information Security Officer (HAM Section 6-1030).

Access to Patient Records





Right to Access

- Individuals have a right to access information about them that is maintained by any health plan or provider in the Department.
- This is also your right. You have the right to access your medical records that your doctor, dentist, or health plan keeps.
- The Department must provide access or make copies of the records it creates or maintains and mail to the individual.



Examples of Department Medical Records

- Claim Detail Report (CDR)
- Treatment Authorization Request (TAR)
- Managed Care Records (premium payments, enrollment records, etc.)
- Medical Case Management Records
- Enrollment/Disenrollment forms
- Application Forms
- Eligibility Records

Who Grants Access?



For Medi-Cal, access will be granted as follows:

EDS	Claim Detail Reports
Medi-Cal Operations	TARS, Medical Case Management, etc.
Managed Care	Managed Care records
Medi-Cal Dental Services Branch	Medi-Cal Dental Records
TPL	CDR information dated back 10 years in microfiche and/or cold storage
Eligibility Division	Eligibility Records

Who May Access Medical Records?

- Individuals (beneficiaries, patients, clients) participating in a health plan or program in the Department will receive an NPP telling them how to access their records.
- A personal representative may also access a patient's records with proper legal authority.

***NOTE:** State laws should be examined by Medi-Cal with regard to minors. See Access Policy for discussion.





Request for Access to Medical Records

- The Department will require that requests for access be in writing using an Access form.
 - Requests for Access by an Individual require a **6236 Access Form**.
 - Requests for Access by a Parent, Guardian or Personal Representative require a **6237 Personal Representative Access Form**.
- The Department:
 - Will respond to individual requests within 30 days after receiving the request.
 - Will require proof of identity and address of requestor.
 - May charge a fee for copying.



Verification of Identity for Telephone Responses

- All individuals requesting information must be verified for right to obtain information.
 - If an individual patient is calling:
 - Ask for information you have available on file such as the Medi-Cal ID card, SSN, date of birth, phone number and address.
 - Use professional judgment when disclosing PHI over the phone.
 - If a provider is calling:
 - Verify that patient belongs to the provider that is calling.



Emergency!

- **If** a program beneficiary is incapacitated and unable to consent,
- **If** there is an emergency requiring immediate care,
AND
- **If** in supervisor's professional judgment disclosure is in the best interest of the beneficiary.
- **Then**, the program may disclose PHI to any of the following over the telephone **without** the beneficiary's consent:
 - A family member, other relative, close friend of the beneficiary.
 - Other person where PHI is directly related to their involvement in care or payment for the beneficiary.

Non-Emergency Situations

- If the patient is not available to consent, then an Authorization Form is needed prior to disclosing information over the telephone to someone else.
 - The person requesting information must provide proof of legal relationship with the Authorization Form
- This applies to advocates or legislative staff acting on behalf of beneficiaries
- This applies to friends and relatives of the patient.





Authorizations

- Authorizations are required for disclosures of PHI to other persons or entities for purposes outside of permitted and required uses and disclosures.
- Individual has a right to revoke a previous authorization.
- Cannot make an individual sign an authorization as a condition for treatment.
- A personal representative may sign for a minor child, incompetent adult, or deceased beneficiary



HIPAA Valid Authorizations

- The authorization form must contain:
 - Description of PHI
 - Who is making request
 - Who the PHI is to go to
 - The purpose for the requested PHI
 - Expiration date of the authorization
 - The signature of the individual whose PHI is being requested
- Valid Authorization Form is the **DHS 6247 Authorization Form**

Amendments to Records





Amendments

- Individuals have a right to request amendments to their records, but the Department is not obligated to accept them.
- If accepted, within 30 days, the Department must:
 - Amend record
 - Inform Individual
 - Inform Others

Denied Amendment Requests



- Requests Denied Must:
 - Be in writing.
 - Include the basis for the denial.
 - Be delivered within 30 days.
- Individual has the right to request that the agency head review the decision.
- Individual has a right to submit a statement disagreeing with the denial.



WHY

Why Would We Deny?

- The Department will deny requests for Amendment if:
 - The record was not created by the Department.
 - The record is not part of the designated record set described by HIPAA and defined by the Department.
 - The record is accurate and complete.

Accounting of Disclosures





Accounting of Disclosures

- The Notice of Privacy Practices (NPP) informs individuals of how we generally may use and disclose their information as allowed or required by law. However, there are certain disclosures that the individual may not be aware of.
- The IPA and HIPAA require the documentation of disclosures that the individual may not be aware of.
 - For example, disclosures required by law to public health or law enforcement



Examples of Accountable Disclosures

The Department must account for PHI/PCI disclosures as follows:

- Court orders, warrants, subpoenas, administrative requests and search warrants
- Breaches or Unauthorized Disclosures, including accidental disclosures
- Accountable Disclosures made by Business Associates
- Public Health disclosures



Examples continued...

- Disclosures made to:
 - Health Oversight Agencies
 - Coroners
 - Public Safety
 - U. S. Dept. of Health and Human Services
 - Research studies
 - Other Governmental Agencies under the Information Practices Act
- Individuals may ask for an Accounting of Disclosures for disclosures made up to six (6) years prior to the request.



Non-Accountable Disclosures

- The following types of disclosures do not need to be accounted for:
 - Treatment, Payment and Healthcare Operations (TPO) as stated on the NPP.
 - Disclosures authorized by the patient or their personal representative.
 - Disclosures to the beneficiary or persons involved with their care or payment of their care.
 - National security or intelligence purposes.
 - Correctional institutions or law enforcement officials having lawful custody of an inmate.
 - Incidental disclosures.
 - Limited data sets used for research purposes.



Details of Accounting

- For each disclosure of PHI the following details should be recorded:
 - Patient Name
 - Patient Number
 - Date of Disclosure
 - Name of person or entity receiving PHI
 - Brief description of information disclosed
 - Purpose of the disclosure
 - Name of who disclosed the information



Sample Accounting Log

Date of Disclosure	Bene Last Name	Bene First Name	ID Number	To Whom Disclosed (Entity, Address, Person, Title)	Information Disclosed	Purpose of Disclosure	Request Received by:
5/2/03	Doe	John	8888888	Immunization Registry, John Smith, Director, 1111 Taylor Road Sacramento, CA 95814	Vaccinations Given	Public Health	S. Jones Analyst
6/7/03	Smith	Jane	5555555	U.S. DHHS Secretary 50 United Nations Bldg San Francisco, CA 94102	Entire Record	Compliance Review	S. Jones Analyst
SAMPLE							

- Each business area must create an Accounting of Disclosures log similar to this sample.
- Privacy Office may request logs at any time.

Complaints About Use, Disclosure, & Protection of Confidential Information



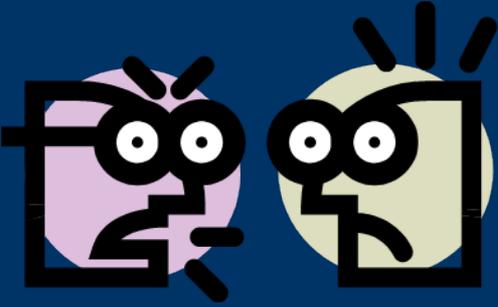
Right to Complain

- HIPAA requires that individuals have a place to complain within the covered entity if they believe PHI has been misused or disclosed inappropriately.
- Individuals have the right to complain about a violation of Privacy or Security policy, whether they are a patient, member of the workforce, or other business associate.
- The complaint must have occurred on or after April 14, 2003.
- HIPAA prohibits retaliatory action against anyone filing a complaint.

Who May Complain?

Any individual whose PHI/PCI the Department maintains, or other persons may file complaints regarding suspected violations of the HIPAA Privacy Rule, including, but not limited to:

- Department Employees
- Business Associate Employees
- Beneficiaries
- Advocates
- Lawyers
- Whistleblowers



Why Complain?

- Complaints may be filed for any of the following:
 - Violating Department Privacy or Security Policies/Procedures.
 - Observing staff misuse PHI/PCI or inappropriately disclosing PHI/PCI.
 - Denial of any Individual Privacy Right under HIPAA (*Example: Denying a patient access to their medical records*).
- The Privacy Office takes all complaints of alleged privacy violations seriously and investigates a variety of complaints regarding suspected misuse, disclosure or disposal of PHI.
- Complaints should be filed on the DHCS Complaint Form (6242)

Breaches of Confidential Information



Responsibility & Prevention

- With the growing rate of identity theft, laws continue to emerge to protect individual's information.
- It is everyone's responsibility in the Department to protect personal confidential information we collect and maintain on individuals in order to avoid breaches of information.



Privacy Breach

- A privacy breach is an unauthorized disclosure of PHI/PCI that violates either federal or state laws.
 - Federal: HIPAA Privacy Rule
 - State: Information Practices Act of 1977
- Privacy breaches may be paper or electronic and may occur when information is transmitted to an unintended recipient.

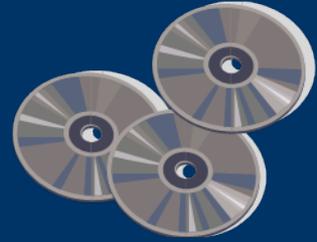
Examples of Paper Breaches



- U
n
a
u
t
h
o
r
i
z
e
d**
- Misdirected paper faxes with PHI/PCI outside of the Department.
 - Loss or theft of paper documents containing PHI/PCI.
 - Mailings to incorrect providers or beneficiaries.
- disclosure**



Examples of Electronic Breaches



- U
n
a
u
t
h
o
r
i
z
e
d
disclosure**
- Stolen, unencrypted laptops, hard drives, PCs with PHI/PCI.
 - Stolen, unencrypted thumb drives with PHI/PCI.
 - Stolen briefcases with unencrypted compact discs containing PHI/PCI.
 - Misdirected electronic fax with PHI/PCI to person outside of state government.



California State Breach Notification Law

- State law requires written notification to California residents whenever there is a breach of unencrypted electronic data containing the following data elements of personal information:
 - The individual's first name or first initial and last name in combination with:
 - Social Security Number
 - Driver's license or California ID number
 - Account number, credit or debit card number in combination with security code, access code or password

AND

- AB 1298 adds two new categories of breach triggering information; effective January 1, 2008
 - Medical information: defined as the individual's medical history, treatment or diagnosis; mental or physical health condition
 - Health information: health insurance policy or subscriber number, application and claims history, as well as appeals records



Reporting Privacy Breaches

- Employees and business associates must take **immediate** action and report (by phone or email) all Privacy Breaches to:
 - Your Supervisor

If your supervisor/manager is unavailable on day of discovery, you are to immediately notify:

 - Privacy Officer
 - Information Security Officer
- Privacy Breaches **DO NOT** include:
 - Misdirected mail within the Department.
 - Emails transmitted from outside the Department to wrong email address within the Department or unencrypted email.



Immediate Action

- The California state law requires the notice to individuals be made “in the most expedient time possible and without unreasonable delay”.
- Staff must take action to report suspected breaches **immediately**.



Notification Letters

- The Department's notification letters to individuals include the following:
 - Advises individuals of steps they can take to protect themselves against possibility of identity theft.
 - Recommends contacting the three credit reporting agencies: Equifax, Experian, and Trans Union.
 - Advises individuals to contact local police or sheriff and file an identity theft report if suspicious activity is found.
 - Contact DMV (Fraud Hotline: 866-658-5758) to place fraud alert on your driver's license.
- California Office of Privacy Protection recommendations for notification letters available at: www.privacy.ca.gov



Fraud Alerts!

- Credit bureau supposed to contact consumer before extending new credit
- Fraud alert can be placed on consumer file at the credit bureaus to alert banks/creditors of potential fraud.
- Contact 3 credit reporting agencies: Equifax, Experian, and Trans Union at toll-free number available 24/7. Alert in place within 72 hours.
- Fraud alert lasts 90 days unless there is evidence of fraudulent accounts. Victim statement extends fraud alert seven years.



Credit Freeze

- California law allows consumers to place a security “freeze” so their credit file cannot be shared with potential creditors.
- Credit freeze is better than a Fraud Alert!
- There is no cost for a credit freeze with a police report filed for victim of identity theft, otherwise \$10 for each credit bureau (\$30).
- Freeze may be lifted to obtain credit with a specific creditor while the freeze is in place.
- Credit bureau must respond within 3 business days.
- Credit freeze is in place until consumer requests that it be removed.



Free Credit Report

One of the best ways for a consumer to protect themselves from identity theft is to monitor their credit history.

- The federal Fair Credit Reporting Act (FCRA) requires the nationwide credit reporting agencies to provide a free copy of their credit report upon request every 12 months.
- A consumer may obtain a free copy of his/her credit report by:
 - Calling toll free at: 1-877-322-8228
 - The three credit bureaus have set up one central website at: <https://www.annualcreditreport.com/cra/index.jsp>.

Note: beware of other sites that may offer “free” credit reports that may charge for other products.

Sanctions and Penalties for Violations of Policy & the Law





Sanctions and Penalties

- HIPAA requires the Department to develop sanctions for employee violations of Privacy and Security Policies and Procedures.
- Sanctions associated with violations of Department Privacy & Security Policies will be pursued within the state disciplinary process.
- There are civil and criminal penalties for violating provisions of the HIPAA Privacy Rule.

State Disciplinary Process

- In order to hold any employee accountable for violation of any policy or procedure, employees must receive adequate training on the policies and procedures.
- State Disciplinary System calls for three phases of discipline:
 - 1) Prevention
 - 2) Corrective Action
 - 3) Disciplinary or Adverse Actions





Civil & Criminal Penalties

- HIPAA civil money penalties apply to covered entities.
 - \$100 for single violation, up to \$25,000 for multiple violations in 1 year.
- Criminal Penalties for knowingly obtaining, using or disclosing PHI in violation of HIPAA.
 - Fine up to \$50,000, imprisonment up to 1 year or both.
 - Under false pretenses, fine up to \$100,000, imprisonment up to 5 years or both.
 - Intent to sell, transfer or use PHI for commercial advantage, personal gain, or malicious harm, fine up to \$25,000, imprisonment up to 10 years, or both.



Liability for HIPAA Violations

- The organization and/or its principal decision makers may be liable for HIPAA penalties.
- Defense: Failure to comply due to reasonable cause and not to willful neglect. Violation corrected within 30 days of knowledge.
- Certain directors, officers & employees of covered entities may be liable for criminal penalties under general principles of corporate criminal responsibility.
- Sufficient that they know the facts that constitute the offense, not necessary to know that the conduct was contrary to the statute or regulations.



HIPAA Criminal Prosecutions

- United States v. Richard W. Gibson
Western District of Washington (Seattle)
Pled guilty August 19, 2004
- United States v. Liz Ramirez
Southern District of Texas (McAllen)
Pled guilty March 6, 2006
- United States v. Fernando Ferrer, Jr. & Isis Machado
 - Southern District of Florida (Ft. Lauderdale)
Indictment announced September 8, 2006

U.S. v. Richard W. Gibson

- Employed by Seattle Cancer Care Alliance
- Obtained name, DOB and SSN of cancer patient
- Applied for credit cards in patient's name
- Charged video games, home improvement supplies, clothes, jewelry, groceries and gasoline
- Total charges: \$9,139.42
- Sentence: 16 months in prison, \$15,569.42 in restitution

U.S. v. Liz Ramirez

- Worked at physician clinic that provided services to FBI agents
- Offered to sell personal and medical info re FBI agent for \$500
- Purchaser was working undercover for FBI
- Ramirez was convicted and imprisoned

U.S. v. Fernando Ferrer, Jr. & Isis Machado

- Machado was a coordinator at a Cleveland Clinic in Naples, Florida
- Per prosecutors, Machado:
 - Printed information from electronic files that included DOB, SSN, & addresses about Medicare patients
 - Then sold info to her cousin Ferrer, owner of Advanced Medical Claims in Naples
 - Information then used to file false Medicare claims, involving 1,100 victims and more than \$2.8 million in claims

U.S. v. Fernando Ferrer, Jr. & Isis Machado

- Both indicted for conspiracy to:
 - wrongfully disclose PHI;
 - commit computer fraud; &
 - commit identity theft
- Also charged with:
 - HIPAA crime of obtaining individually identifiable health information with intent to sell, transfer and use for personal gain (the ten year felony);
 - fraud in connection with computers (18 U.S.C. § 1030);
 - five counts of aggravated identity theft (18 U.S.C. § 1028)



Information Practices Act

(Civil Code Section 1798.55)

- Intentional violation of any provision of the IPA by an employee of the agency is a cause for discipline, including termination.
- Misdemeanor for requesting or obtaining any record containing PCI under false pretenses.
- Fine: Up to \$5,000 or imprisonment, up to 1 year, or both.



Examples of Employee Violations

- Employee discusses the name of a beneficiary with friends.
- Employee uses PHI to Send a Birthday Card.
- Employee sells names and addresses from MEDS or any system containing confidential information to a Marketing Firm.
- Employee gets confidential medical information from MEDS about an ex-spouse and uses or discloses it for personal reasons.

Website References

- Please print the next two screens as a resource to find manuals, documentation, and forms that have been referenced in this presentation.
 - DHCS Privacy Office website at:
<http://www.dhs.ca.gov/privacyoffice/>
 - Information Security Office website at:
<http://itsd.int.dhs.ca.gov/4%20Information%20Security/>
 - Health Administrative Manual:
<http://admin.int.dhs.ca.gov/ham/>
 - State Administrative Manual:
<http://sam.dgs.ca.gov/TOC/>

Website References

- Notice of Privacy Practices on the Privacy Office website at:
<http://www.dhs.ca.gov/privacyoffice/NPP/>
- Access (DHS 6236), Amendment (DHS 6238), Accounting of Disclosures (DHS 6244), Complaints (DHS 6242) and Authorization (DHS 6247) forms are available on the Privacy Office website at:
<http://www.dhs.ca.gov/privacyoffice/forms/>
- The Privacy Breach Report is available on the Privacy Office website at:
<http://www.dhs.ca.gov/privacyoffice/Breaches/Breach%20Written%20Report%20Outline.doc>
- Department of Health & Human Services FAQ:
<http://www.hhs.gov/hipaafaq/>
- Office for Civil Rights HIPAA Homepage (Privacy & Security Rules):
<http://www.hhs.gov/ocr/hipaa/>
- Centers for Medicare and Medicaid Services Homepage:
<http://www.cms.hhs.gov/>

The End

- If you have any questions, please contact one of the following:

DHCS Privacy Officer

E-mail: privacyofficer@dhcs.ca.gov

Phone: (916) 440-7750

FAX: (916) 440-7710

CDPH Privacy Officer

E-mail: privacyofficer@dhcs.ca.gov

Phone: (916) 440-7432

Information Security Officer

E-mail: SECADMIN@dhcs.ca.gov

Phone: (916) 440-7000 or

(800) 579-0874