EMERGING TRENDS IN PRIVACY AND INFORMATION SECURITY.

Presented by Marti Arvin
Chief Compliance Officer
UCLA Health Sciences

AGENDA

- Brief discussion of where we have been and where we are going
- Discussion of Federal Enforcement Actions
- Privacy and Security issue to think about in your organization

WHERE HAVE WE BEEN

- For a number of years there was not a heavy emphasis by organizations on privacy and information security of sensitive information.
- The explosion of health information stored and exchanged in electronic format has increased the concern about privacy and security

WHERE HAVE WE BEEN

- Once the HIPAA final regulations were passed oversight has increased
- However with the limited enforcement by OCR and CMS it was something that many organizations might not have given the same focus comparable to other aspects of its compliance program

WHERE HAVE WE BEEN

- Privacy and Information Security Officers
  - May organizations identified someone as their privacy officer and/or information security officer
  - This was not always a component of the compliance office
  - The person identified in this role might not have been a person on a “high” level of authority when it was a separate office

WHERE ARE WE GOING

- Increased enforcement is becoming the norm
- Started in the mid 2000s with complaint driven enforcment by OCR
- Now enforcement by routine reviews, review of headlines, complaints, etc
- OCR is increasing their staff for enforcement purposes
- OCR has and plans to continue to use resolution agreements as an enforcement tool
- What about FCA liability?

FEDERAL ENFORCEMENT ACTIONS: PROVIDENCE HEALTH & SERVICES

- On July 16, 2008, Providence entered into a resolution agreement with OCR whereby it agreed to pay $100,000 and implement a detailed Corrective Action Plan (CAP) to settle complaint stemming from its loss of unencrypted backup media and laptops in 2005 and 2006
- The CAP requires:
  - Revising policies and procedures regarding physical and technical safeguards (e.g., encryption) governing off-site transport and storage of electronic media containing patient information, subject to HHS approval;
  - Training workforce members on the safeguards;
  - Conducting audits and site visits of facilities; and
  - Submitting compliance reports to HHS for a period of three years.

* This agreement was pre-HITECH

FEDERAL ENFORCEMENT ACTIONS: CVS PHARMACY

- January 16, 2009, CVS accepted $2,250,000 penalty and Corrective Action Plan (CAP) to settle complaint stemming from its practice of disposing of old prescriptions and prescription bottles
- The CAP requires:
  - Revising and distributing its policies and procedures regarding disposal of protected health information;
  - Sanctioning workers that do not follow the policies and procedures;
  - Training workforce members on these new requirements;
- Subsequently, OCR issued PHI Disposal FAQs

FEDERAL ENFORCEMENT ACTIONS: RITEAID PHARMACY

- June 7, 2010, Rite Aid accepted $1,000,000 penalty and Corrective Action Plan (CAP) to settle complaint stemming from its practice of disposing of sensitive information in an improper manner.
- The CAP requires:
  - Designate a compliance representative for the CAP
  - Revising and distributing its policies and procedures regarding disposal of protected health information;
  - Sanctioning workers that do not follow the policies and procedures;
  - Training workforce members on these new requirements and annually for the term of the resolution agreement;

FEDERAL ENFORCEMENT ACTIONS: RITEAID PHARMACY

- The CAP requirements cont.:
  - Conducting internal monitoring;
  - Engaging a qualified, independent third-party assessor to conduct assessments of Rite Aid's compliance with the requirements of the CAP and render reports to HHS;
  - New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
  - Submitting compliance reports to HHS for a period of three years.

CIGNET ENFORCEMENT

- The organization failed to respond to the request for records from 43 individuals
- The individuals complained to OCR.
- OCR requested records from the organization
- The organization did not respond
- When they did respond they send records for 4500 patients that OCR did not request
- The fine was for the failure to respond to the patients and to OCR

CIGNET ENFORCEMENT

- Fine breakdown
  - Failing to respond to the patients - $1,351,000
  - Failing to respond to OCR - $3,000,000
    - Would have been $373,900,000 without annual cap of $1,500,000
- Bad news
  - Each day was a separate violation
- Good news they did not count failure to supply data to OCR for each patient as a violation of a separate standard subject to the $1,500,000 cap
  - Fine would have been $60,000,000

MASS GENERAL HOSPITAL RESOLUTION AGREEMENT

- Employee lost records of 192 patients on subway.
  - Pt name, DOB, MRN, some HIV information was lost
- February 14, 2011, Massachusetts General Physicians Organization entered into a Resolution Agreement/CAP with HHS and agreed to pay $1,000,000.
- CAP obligations include:
  - Policies and Procedures
  - Training
  - Monitoring
  - Reporting

MANAGEMENT SERVICES ORGANIZATION WASHINGTON

- Investigation by OCR was based on a referral from OIG & DOJ civil division
- Allegation was the improper disclosure of EPHI for marketing Medicare Advantage plans without a valid authorization from 2007 to 2010
- December 13, 2010, MSOW entered into a Resolution Agreement/CAP with HHS and agreed to pay $35,000.

MANAGEMENT SERVICES ORGANIZATION WASHINGTON

- CAP obligations include:
  - Policies and Procedures
  - Training
  - Monitoring
  - Reporting
- Term of CAP is 2 years

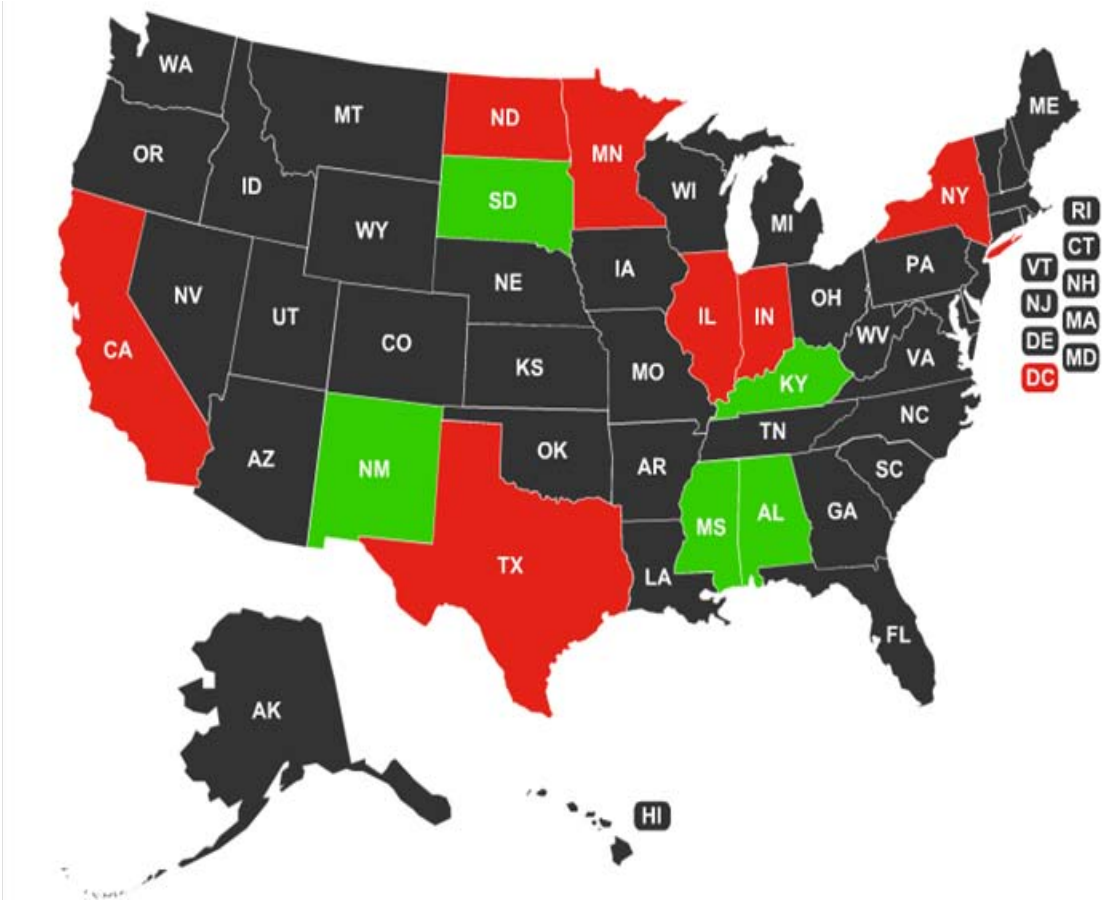
POST-HITECH: FIRST REPORTED STATE ENFORCEMENT - *CT V. HEALTH NET*

- **Complaint Allegations:**
  - May 2009 - Health Net learns of lost portable disc drive with financial and PHI information of approx. 446,000 current and former CT enrollees.
  - November 2009 – Health Net notifies CT enrollees.
- **January 2010 - CT AG files suit:**
  - **3 Causes of Action Pled:**

1. Failure to comply with HIPAA.
2. Violation of CT Unfair Trade Practices Act.
3. Civil Penalties for Willful Violation of CT Unfair Trade Practices Act.

- **Relief Sought:**
  - **Injunctive relief under HIPAA and CT State law; Statutory damages for HIPAA violations, including costs and attorneys fees under HITECH; State CMPs (up to $5,000 per willful violation) and attorneys fees and costs under CT State law.**

Available at http://law2point0.com/wordpress/2009/09/15/50-state-security-breach-notice-law/



Red – Acquisition Based

Black – Risk Based

Green -- None

STATE SECURITY BREACH NOTIFICATION REGULATIONS

RECENT FEDERAL ACTIVITY

- Kerry/McCain bill proposed in April 2011
- Obama administration proposed legislation – May 2011

KERRY/MCCAIN BILL

- Key highlights
  - Who is covered?
    - Entities that collect, use, transfer or store covered information of >5000 persons during a consecutive 12 month period and
    - Is subject to FTC authority
    - Is common carrier subject to the Communications Act or
    - Is a non-profit, including 501(c) organizations

KERRY/MCCAIN BILL

- Kerry/McCain bill proposed in April 2011
- Key highlights
  - Defines covered information as
    - Personally identifiable information
      - Identified as first name or initial and last name
      - Postal address
      - Email address
      - Phone number
      - SSN
      - Credit card account number
      - Unique if it alone can be used to ID person
      - Biometric data

KERRY/MCCAIN BILL

- Kerry/McCain bill proposed in April 2011
- Key highlights
  - Defines covered information as
    - Personally identifiable information also includes the following if combined with one of the items on the prior slide
      - DOB
      - Birth or adoption certificate #
      - Place of birth
      - Unique ID that cannot alone identify the individual
      - Precise geographic information but not IP address

KERRY/MCCAIN BILL

- Key highlights continued
  - Defines covered information as (cont.)
    - Unique identifier information
    - Any information collected, used or stored in connection with personally identifiable or a unique ID that that can reasonable be used to ID a specific individual

KERRY/MCCAIN BILL

- Key highlights continued
  - Defines sensitive personally identifiable information as
    - PII that if lost, compromised or disclosed without authorization carries significant risk of economic or physical harm
    - Information related to a
      - specific medical conditions
      - Religious affiliations

KERRY/MCCAIN BILL

- Key highlights continued
  - Offer an opt-out provision for individuals
  - Preempts state laws that cover the same information except state laws regarding
    - Protection of financial information & medical information
    - Breach notification
  - Entities covered by HIPAA, FERPA, GLBA, COPPA, FCRA and/or CALEA would be exempt from the act to the extent the other laws apply
  - Requires notice of privacy practices
  - Penalties
    - A entity that knowingly and repeatedly violates can be subject to $16,500 CMP for every day the entity is in violation not to exceed $3,000,000

PRESIDENT'S LEGISLATION

- Requires breach notification
- Applies to any organization, corporation, trust partnership, sole proprietorship, unincorporated, or venture established to make a profit or nonprofit
- Sensitive personally identifiable information in digital or electronic form
  - First name (or initial) & last name combined with any two of the following:
    - Home address or telephone number
    - Mother's maiden name
    - DOB
  - Full SSN, DL number, passport number, alien registration number or any other unique gov. ID

PRESIDENT'S LEGISLATION

- Sensitive personally identifiable information (cont.)
  - Unique biometric data including fingerprint, voice print, retina or iris image or any other unique physical representation
  - Unique account ID such as financial acct number, credit or debit acct number, electronic ID, user name or routing code or
  - Combination of the following data elements
    - First name or initial and last name
    - Unique acct ID or
    - Any security code, access code, or password or source code that could generate such codes or passwords

PRESIDENT'S LEGISLATION

- Applies to business entities that uses, accesses, transmits, stores, disposes of or collects sensitive PII about more than 10,000 individuals during a 12 month period shall notify individuals of a data breach that has been or is reasonable believed to have been accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual.
- Notice must be without unreasonable delay not to exceed 60 days unless the business entity request extension from FTC.

PRESIDENT'S LEGISLATION

- No notice requirement if data is rendered unusable, unreadable, or indecipherable through security technology or methodology generally accepted by experts in the field of information security
  - Probably would mean encryption
- If you don't notify based on the above exception you must notify FTC within 45 days of your risk assessment
  - Failure to perform a risk assessment would violate the law

PRESIDENT'S LEGISLATION

- Notice
  - Can be done via mail, phone or email
  - If more than 5000 persons
    - Notice to the media would be required
    - Must also notify credit reporting agencies
  - Content of the notice is defined
- Allows for enforcement by State Attorneys General
- Act does not apply to covered entities and business associates covered by HITECH
- Preempts state laws

FEDERAL FINES AND PENALTIES

- HIPAA penalty ranges are
  - $100 up to cap of $1,500,000 for violations of each identical requirement or prohibition
  - $1,000 up to cap of $1,500,000 for violations of each identical requirement or prohibition
  - $10,000 up to a cap of $1,500,000 for violations of each identical requirement or prohibition
  - $50,000 up to a cap of $1,500,000 for violations of each identical requirement or prohibition

IMPORTANT DEFINITIONS

- Reasonable diligence would be defined as ‘‘the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.’’
- Willful neglect is ‘‘conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.’’

IMPORTANT DEFINITIONS

- ‘‘Reasonable cause’’ would be defined as ‘‘circumstances that make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.’’

WHAT DETERMINES WHICH PENALTY WILL BE IMPOSED?

- If the violation is one that the covered entity did not know about and with the exercise of reasonable diligence would not have known about the Secretary has the discretion to impose the $100 penalty up to the $50,000 penalty
  - What type of circumstance could this be?

WHAT DETERMINES WHICH PENALTY WILL BE IMPOSED?

- If the violation is determined to be a reasonable cause and not willful neglect then the penalty range starts at $1,000 and can go up to $50,000 per violation
- If the violation is due to willful neglect and the covered entity corrects it within 30 days of discovery the penalty range starts at $10,000 and can go up to $50,000 per violation

WHAT DETERMINES WHICH PENALTY WILL BE IMPOSED?

- If the violation is due to willful neglect and the covered entity does not correct it within 30 days of discovery the penalty range starts at $50,000 per violation
- A violation is deemed to be discovered when the covered entity knew or by exercise of reasonable diligence should have known that the failure to comply occurred.

THINGS TO THINK ABOUT

- What can create liability
  - Failure to have a BAA in place when one is required.
  - Improper use of disclosure of PHI for research purposes

FAILURE TO HAVE A BAA IN PLACE WHEN ONE IS REQUIRED

- If you know you needed a BAA and you did not get one for 6 months
- Is the failure to correct due to willful neglect?
  - conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.
    - You knew you needed it
  - Can you argue that you were trying to get BAA in place?
  - Does it matter if you shared PHI with the BA without the BAA in place while you were negotiating?

SHARING DATA WITH THIRD PARTIES

- Business Associates and ensuring that Business Associate Agreements are executed prior to the sharing of data
- Who is responsible?
  - Purchasing
    - Hospital purchasing
    - Campus purchasing
  - Legal
  - Compliance

BUSINESS ASSOCIATES

- Who can enter an agreement with a third party?
  - Hospital purchasing
  - Campus purchasing
  - Department leaders
- How do you ensure that individuals who can enter agreements know when a BAA is necessary?
- How do you audit to help ensure BAAs are in place when necessary?

USE AND DISCLOSURE OF DATA IN RESEARCH

- Ways to use and disclose PHI for Research
  - With an authorization
  - Waiver of authorization
  - Allegedly de-identified data sets

COMPLIANCE ISSUES WITH USING AND DISCLOSING PHI FOR RESEARCH

- When the IRB indicates an authorization is required
  - No oversight by the IRB to ensure
    - an authorization is obtained.
    - The authorization used covers the necessary uses and disclosures of PHI for the research project
  - Unclear where the research authorization should be stored if obtained
  - Continued misunderstanding by researchers regarding the distinction between
    - PHI and RHI
    - Informed consent and authorization

USE AND DISCLOSURE OF DATA IN RESEARCH

- Under a waiver of authorization
  - What information is provider to the IRB?
    - Does the IRB understand its obligations to determine if a waiver is appropriate?
    - The rule makes it the responsibility of the IRB to ensure the criteria for the waiver is met and to determine what PHI can be used for the research project
    - The criteria for waiver of an authorization is the same for both the complete and partial waiver

WAIVER OF THE AUTHORIZATION

1. An authorization can be waived if the IRB determines
   A. The use or disclosure of the PHI involves no more than minimal risk to the privacy of the subject based on at least all of the following:

1. An adequate plan to
   i. protect the identifiers
   ii. destroy the identifiers at the earliest possible time
2. Adequate written assurance the PHI will not be reused or re-disclosed except under very limited circumstances
   i. Required by law
   ii. Oversight of the research
   iii. Other research after additional IRB approval

WAIVER OF AUTHORIZATION (CONT.)

2. The research cannot practicably be done without the waiver of authorization
    a. Why won't other recruitment methods be effective in the case of partial waiver?
    b. Why is obtaining an authorization impractical?
        a. Example: retrospective records review of clinical database for ER visits for patients with gunshot wound to the head
3. The research cannot practicably be done without access to the PHI
    a. Why must the researcher access identifiable information for his/her study?

COLLECTING MORE INFORMATION THAT AGREED TO IN A WAIVER OF AUTHORIZATION

- Researcher's states in waiver request approved by IRB that only MRN and date of service will be collected.
- Actually collects name, SSN, DOB, Date of service and MRN with medical information.

USING AND DISCLOSING DE-IDENTIFIED DATA

- If a researcher asserts that he/she is only collecting de-identified data there is no Common Rule oversight however HIPAA continues to apply if the researcher is reviewing identified data to create his/her de-identified data set.
- Does your IRB understand the distinction?
  - Would your IRB review this research or count it as exempt?
  - Does the researcher understand the need to comply with HIPAA to look at the information?

STORAGE OF INFORMATION IN A RESEARCH PROJECT

- Does the researcher understand that if the data is stored outside of the covered component of our hybrid entity it still needs protection?
- Because HIPAA does not apply does not mean no rules apply.
- Co-mingling of clinical and research data.

ELECTRONIC HEALTH RECORDS

- Using and disclosing data within the covered component
  - Role based access
    - Distinction between legacy system and new system
    - Upgrades to existing system
  - Minimum necessary
    - Break the glass features

ELECTRONIC HEALTH RECORDS

- Using and disclosing data with external parties
  - Community physician practices
  - CareEverywhere
  - Researchers
  - External reviewers

QUESTIONS