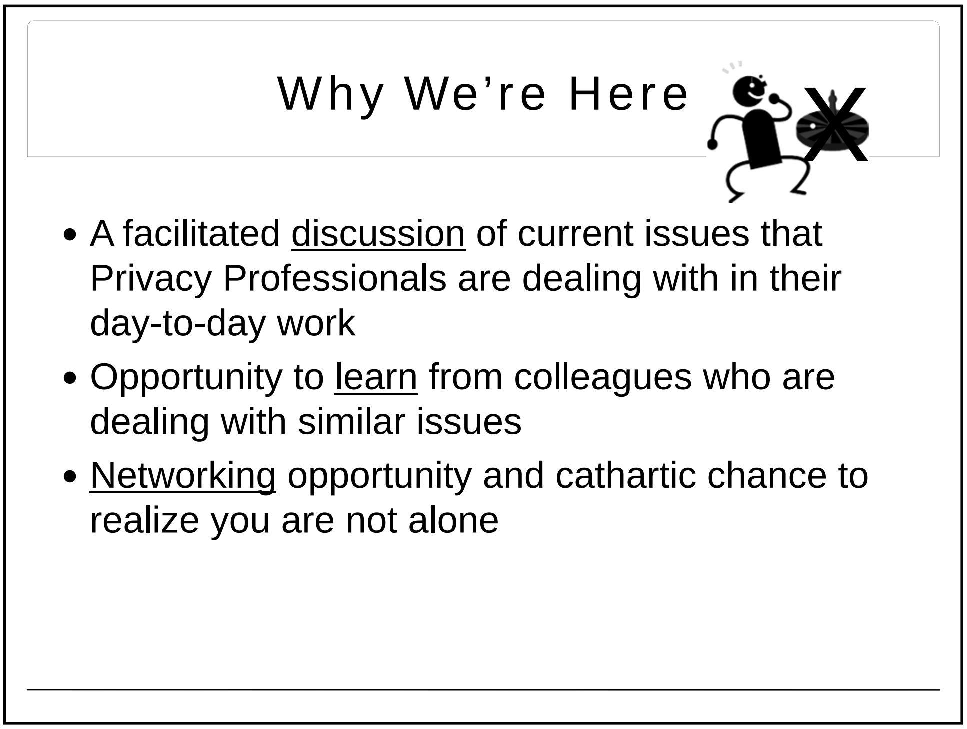
HCCA Institute Privacy Officer Round Table Discussion

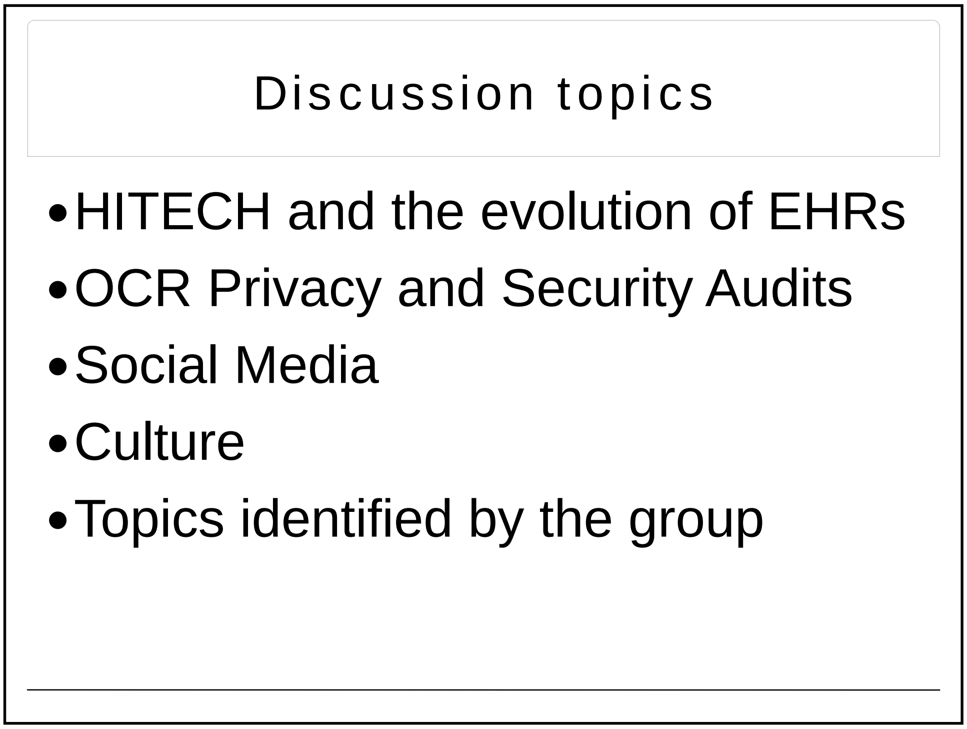
Marti Arvin

Deann Baker



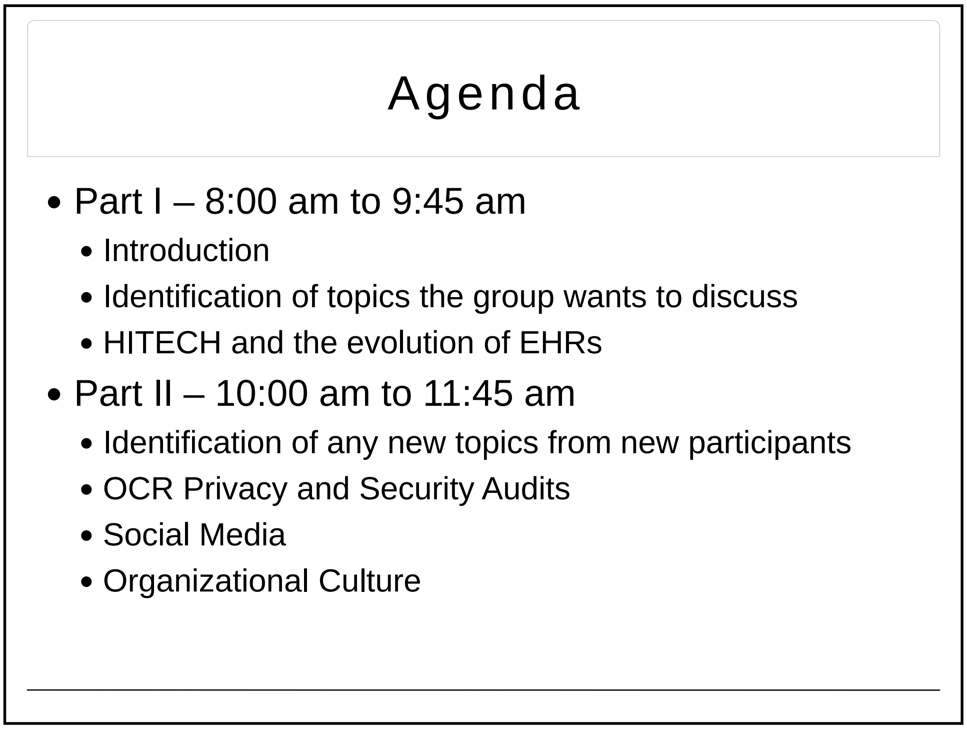
Why We're Here

- A facilitated discussion of current issues that Privacy Professionals are dealing with in their day-to-day work
- Opportunity to learn from colleagues who are dealing with similar issues
- Networking opportunity and cathartic chance to realize you are not alone



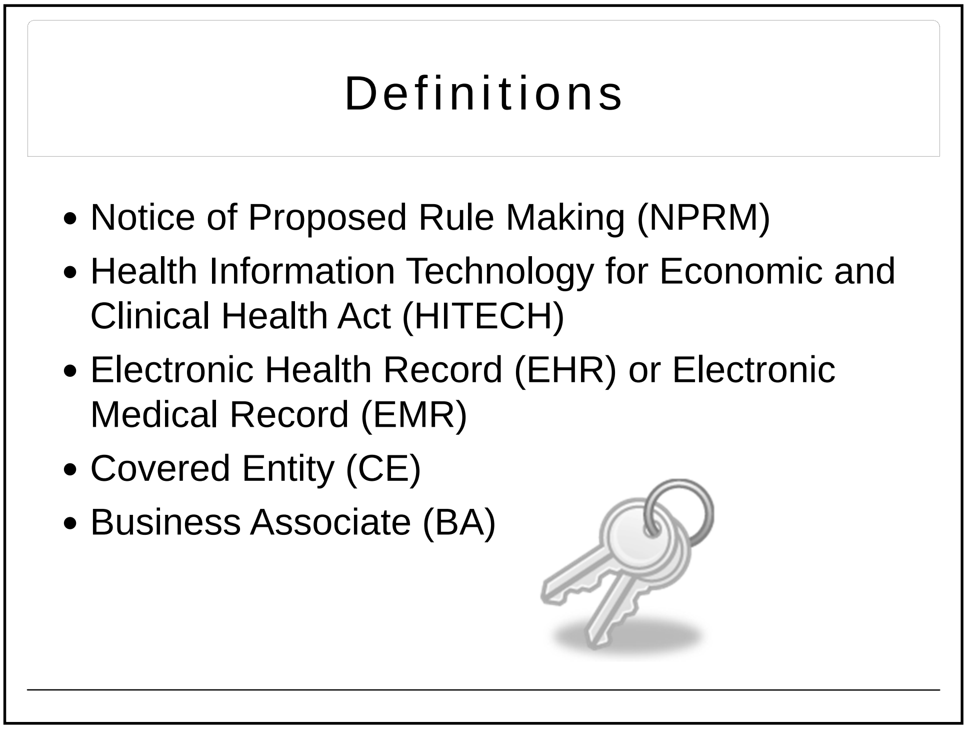
Discussion topics

- HITECH and the evolution of EHRs
- OCR Privacy and Security Audits
- Social Media
- Culture
- Topics identified by the group



Agenda

- Part I – 8:00 am to 9:45 am
  - Introduction
  - Identification of topics the group wants to discuss
  - HITECH and the evolution of EHRs
- Part II – 10:00 am to 11:45 am
  - Identification of any new topics from new participants
  - OCR Privacy and Security Audits
  - Social Media
  - Organizational Culture



Definitions

- Notice of Proposed Rule Making (NPRM)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Electronic Health Record (EHR) or Electronic Medical Record (EMR)
- Covered Entity (CE)
- Business Associate (BA)

HITECH Act & Evolution of EHR

Discussion

HITECH/EHR Checklist

Items to be discussed:

- Enforcement
- Data Breach reporting
- Restrictions
- Accounting/Access
- Auditing/Access
- Marketing/Fundraising
- Enforcement activities

Considerations:

- Dates
- Interim Rules
- State Laws

Enforcement

- When your breach occurred may be important?
- Did it occur before the increase to the CMPs in February 2009?
  - OCR will apply the old CMPs to old breaches and the new CMPs to new breaches
  - As we get further from the February 2009 date this will matter less but you should be aware of it.

Breach Checklist

- State Law impacts
- Roles and Responsibilities
- Risk Assessment activities
- Reporting and disclosure processes
- Managing activities and response
- Policies & procedures
- Sanctions of work force
- Internal process

Internal Checklist

1. Communication plan:
   - senior management, board members, legal department, risk management, IT, and marketing or others
2. Initial action plan:
   - determine who does what activities based on expertise
   - manage internal and external inquiries (communication)
3. Investigation and risk assessment activities:
   - what information was lost, disclosed, intercepted, or altered
   - what occurred, how and why, and potential liability

Internal Checklist

6. External notification:
- enforcement agencies and patients
- timelines to be considered based on what and when you know
- determine how to send the notifications based on what you learn

7. Response plan to inquiries after notification:
- litigation (determine who the contact will be)

8. Corrective action plans:
- remediate damages
- audit and monitor

Breach Checklist

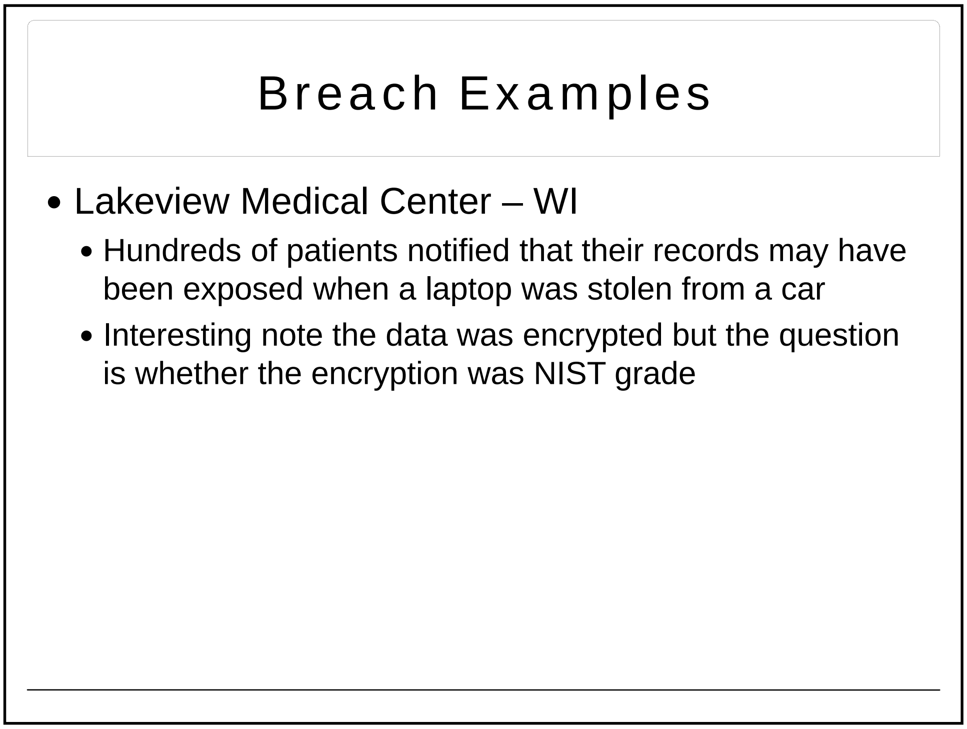
- Individual Notice
- Media Notice
- Notice to the Secretary
- Notice to BA
- Burden of Proof
- Resources: http://www.google.com/search?q=HITECH+Access+-accounting+of+disclosures&rls=com.microsoft%3A*%3AIE-SearchBox&oe=UTF-8&sourceid=ie7&rlz=1I7ADFA_enUS395&safe=active&oq=HITECH+Access+-accounting+of+disclosures&aq=f&aqi=&aql=&gs_sm=3&gs_upl=39327l54842l0l55108l42l41l3l28l0l1l343l2233l0.2.6.1l9l0

Breach Examples

- Stanford Health –
  - external vendor shared a file with a prospective applicant who then posted on a site asking if anyone could help him create graphs from the data
- UCLA Health System
  - Stolen hard drive
- Sutter Health –
  - Unencrypted device with information 4.2 million patients was stolen

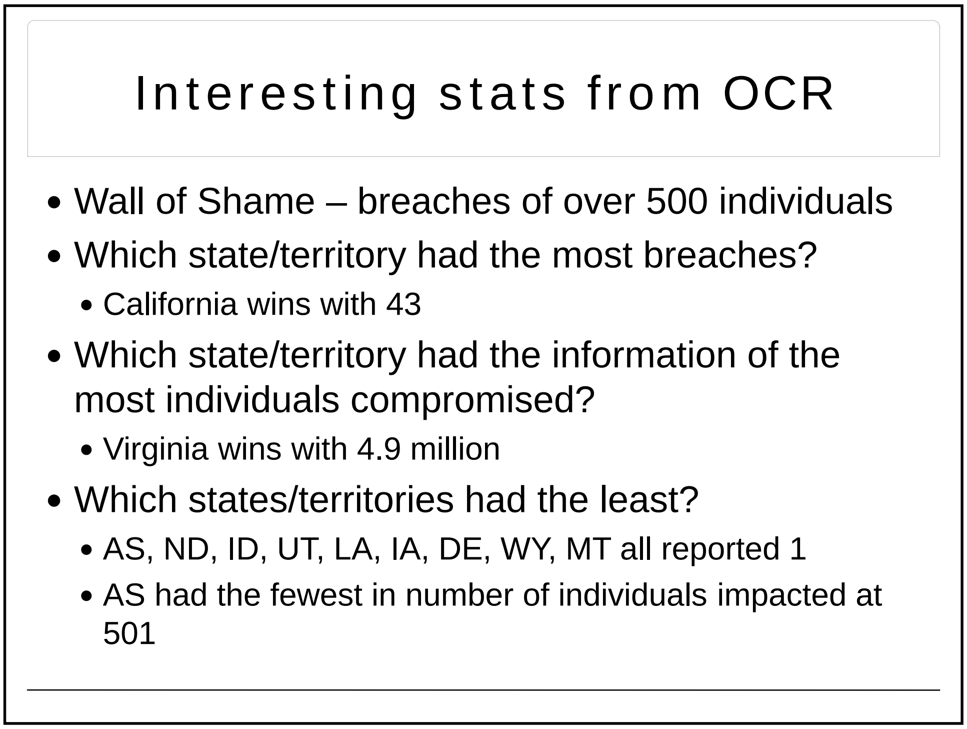
Breach Examples

- February 2012 records from Dashy Medical Center in New York found scattered on the sidewalk.
- St. Joseph Health – Orange county CA
  - notified 32000 patients that their records may have been searchable on the internet.
  - The hospital became aware of the breach when a patient’s attorney contacted them.



Breach Examples

- Lakeview Medical Center – WI
  - Hundreds of patients notified that their records may have been exposed when a laptop was stolen from a car
  - Interesting note the data was encrypted but the question is whether the encryption was NIST grade



Interesting stats from OCR

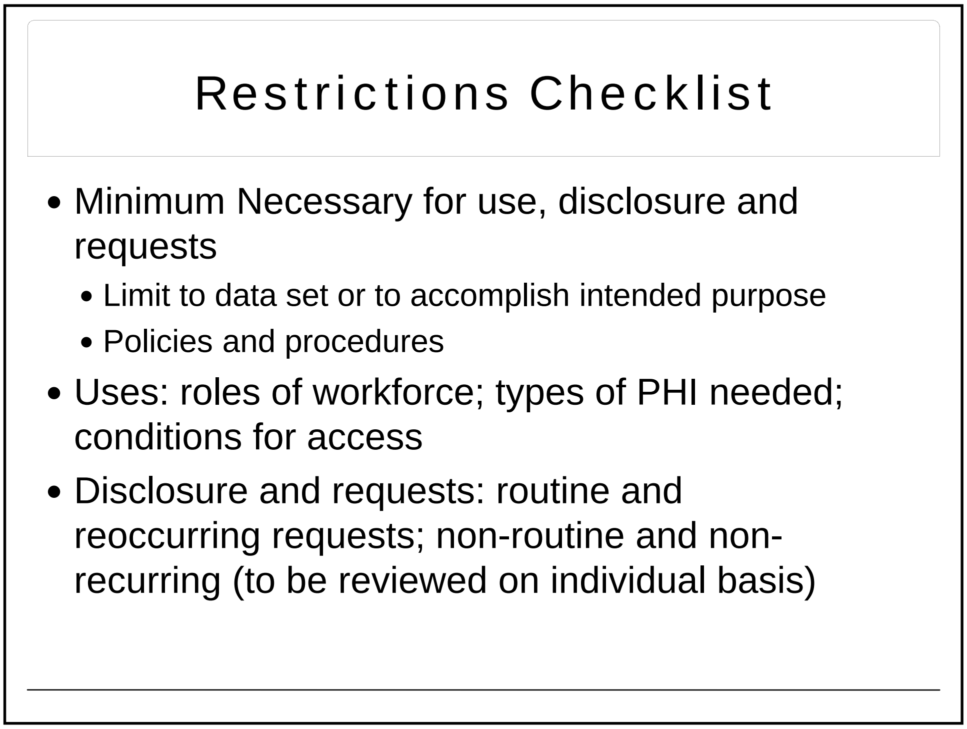
- Wall of Shame – breaches of over 500 individuals
- Which state/territory had the most breaches?
  - California wins with 43
- Which state/territory had the information of the most individuals compromised?
  - Virginia wins with 4.9 million
- Which states/territories had the least?
  - AS, ND, ID, UT, LA, IA, DE, WY, MT all reported 1
  - AS had the fewest in number of individuals impacted at 501

Interesting stats from OCR

- What are the top five reasons for the compromise of the data
  - Number 1 is theft
    - Over 50% of the incidents
  - Number 2 is Unauthorized access/disclosure
  - Number 3 is Loss
  - Number 4 is Hacking/IT incident
  - Number 5 is Improper Disposal

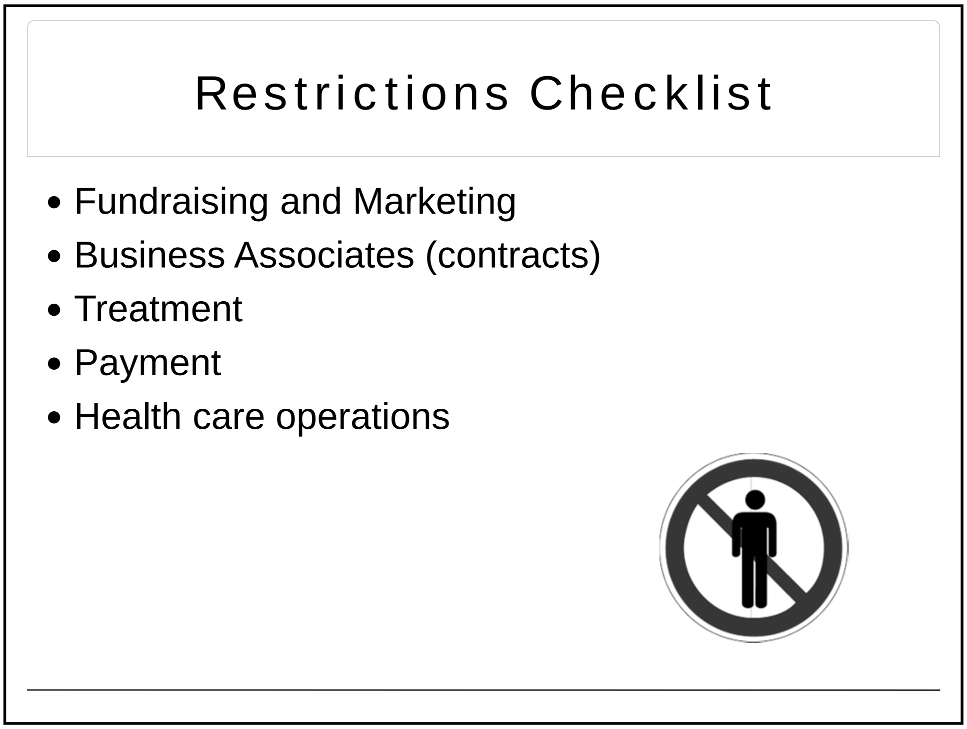
Identity Theft

- According to ID Experts
  - Medical identity theft is estimated to cost $234 billion annually based on FBI estimates
- The street value of a stolen medical identity is approximately $50 according to the World Privacy Forum
- Roughly 1.4 million Americans were victims of medical identity theft in 2010 according to a study done by Ponemon Institute
- The same report estimated the annual economic impact to be $30.9 billion



Restrictions Checklist

- Minimum Necessary for use, disclosure and requests
  - Limit to data set or to accomplish intended purpose
  - Policies and procedures
- Uses: roles of workforce; types of PHI needed; conditions for access
- Disclosure and requests: routine and reoccurring requests; non-routine and non-recurring (to be reviewed on individual basis)



Restrictions Checklist

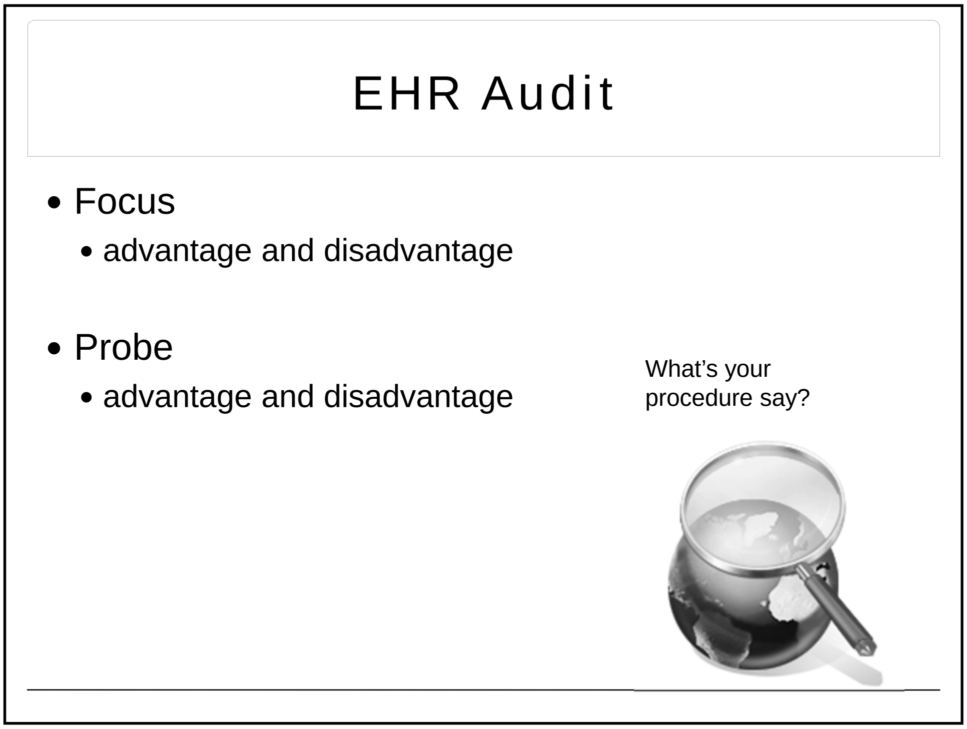
- Fundraising and Marketing
- Business Associates (contracts)
- Treatment
- Payment
- Health care operations

Accounting Checklist

- Accounting of disclosures to Certain Information in Electronic Format
- TPO
  - CEs with EHRs - date dependent
  - BA requirement
- Uses

EHR Audit

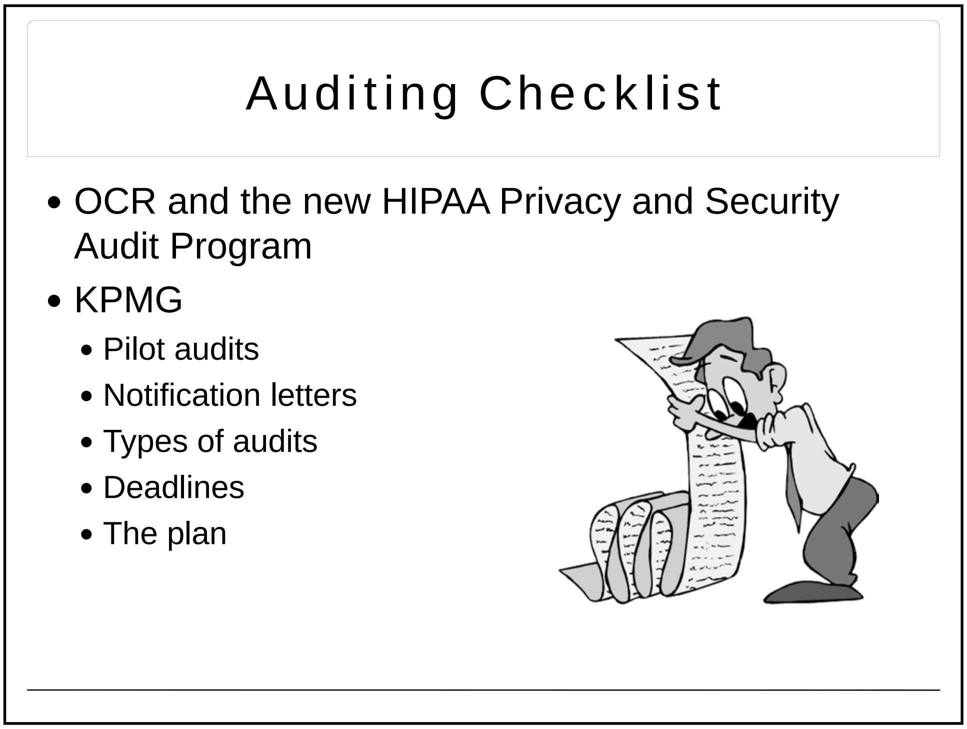
- Auditing and Monitoring reports
  - same last name
  - same name
  - same name chart modification
  - VIP of Person of Interest
  - Break the glass functionality



EHR Audit

- Focus
  - advantage and disadvantage
- Probe
  - advantage and disadvantage

What’s your procedure say?



Auditing Checklist

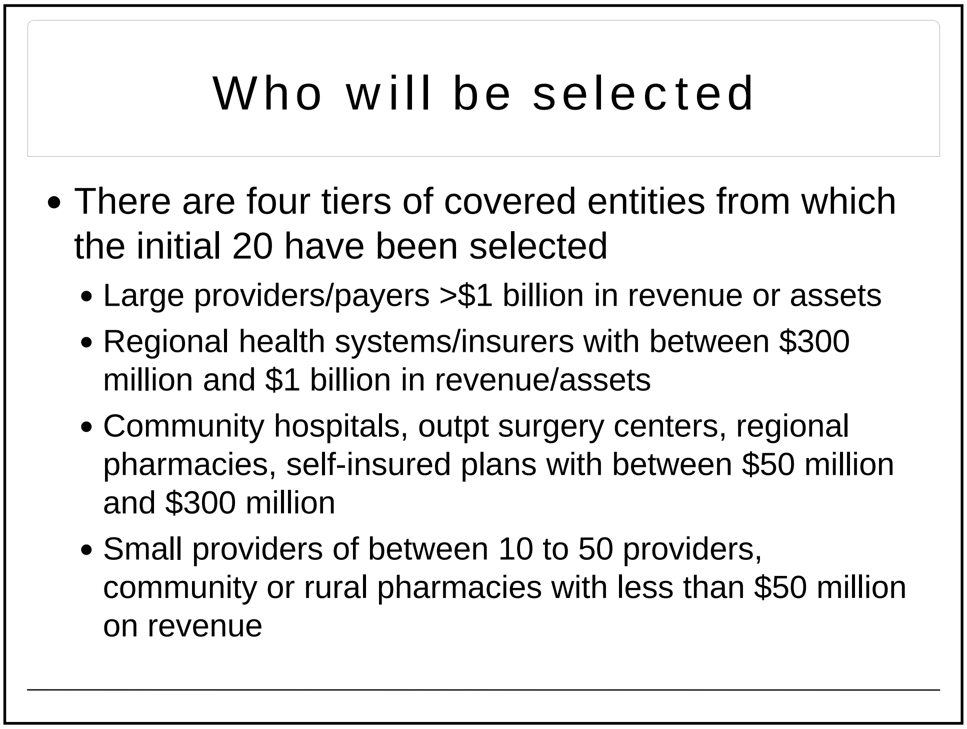
- OCR and the new HIPAA Privacy and Security Audit Program
- KPMG
  - Pilot audits
  - Notification letters
  - Types of audits
  - Deadlines
  - The plan

OCR Privacy and Security Audits

- HITECH specifically provides that OCR will conduct period audits
- The OCR initially contracted with Booz Allen to identify the universe of covered entities that are candidates for potential audits
- Then contracted with KPMG to conduct 150 privacy and security audits in 2012

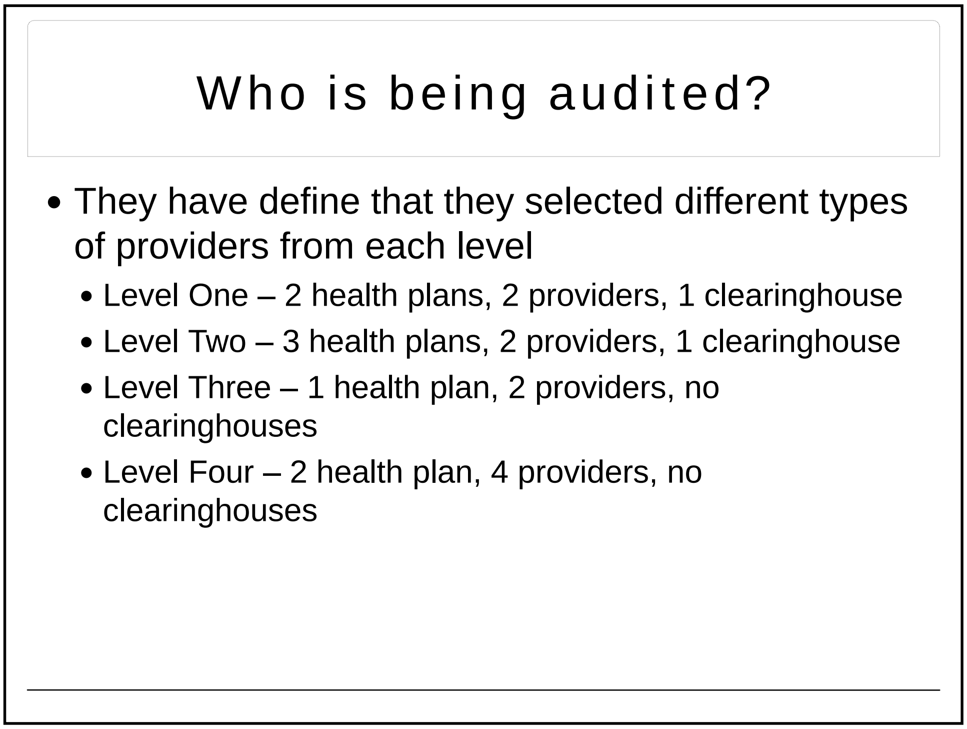
When will this be done?

- An initial audit of 20 entities to be done by the end of March 2012.
- The remaining 130 will be done between April and December of 2012
- Business associates will not likely be audited in this process



Who will be selected

- There are four tiers of covered entities from which the initial 20 have been selected
  - Large providers/payers >$1 billion in revenue or assets
  - Regional health systems/insurers with between $300 million and $1 billion in revenue/assets
  - Community hospitals, outpt surgery centers, regional pharmacies, self-insured plans with between $50 million and $300 million
  - Small providers of between 10 to 50 providers, community or rural pharmacies with less than $50 million on revenue



Who is being audited?

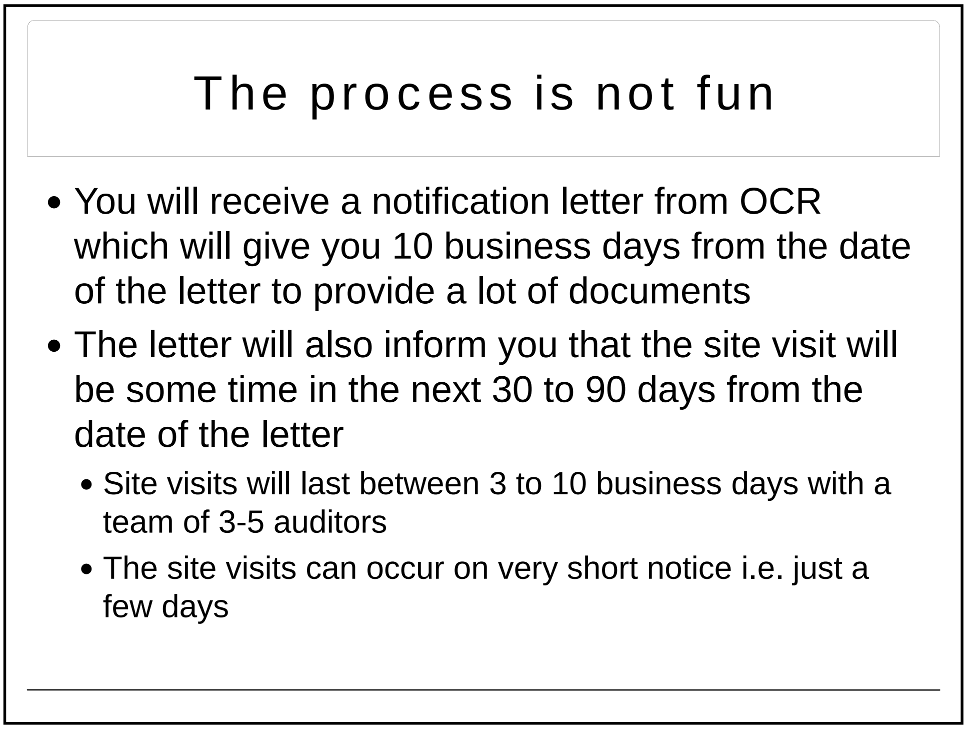
- They have define that they selected different types of providers from each level
  - Level One – 2 health plans, 2 providers, 1 clearinghouse
  - Level Two – 3 health plans, 2 providers, 1 clearinghouse
  - Level Three – 1 health plan, 2 providers, no clearinghouses
  - Level Four – 2 health plan, 4 providers, no clearinghouses

The first 20

- There are eight health plans
  - 1 medicaid health plan
  - 1 SCHIP plan
  - 3 group health plans
  - 3 health insurance issuers
- There are 12 providers
  - 3 physician groups
  - 3 hospitals
  - 1 lab
  - 1 dental practice
  - 2 Nursing home
  - 1 pharmacy

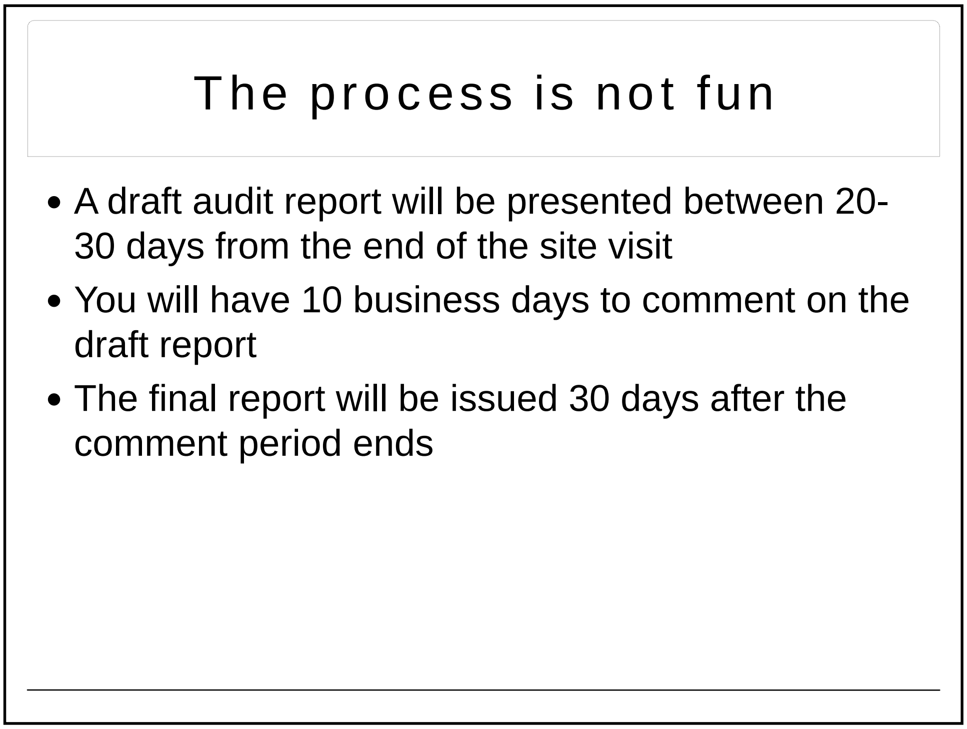
What are they looking for in the audit?

- Do you have implemented Privacy and Security policies and procedures
- Are you following the breach notification rule



The process is not fun

- You will receive a notification letter from OCR which will give you 10 business days from the date of the letter to provide a lot of documents
- The letter will also inform you that the site visit will be some time in the next 30 to 90 days from the date of the letter
  - Site visits will last between 3 to 10 business days with a team of 3-5 auditors
  - The site visits can occur on very short notice i.e. just a few days

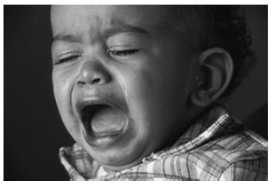


The process is not fun

- A draft audit report will be presented between 20-30 days from the end of the site visit
- You will have 10 business days to comment on the draft report
- The final report will be issued 30 days after the comment period ends

More good news

- The audits are intended to be preventative and not punitive
- If there is a serious finding it may result in an OCR compliance review
- What does all this mean?
  - Be prepared



Social Media

Discussion

Social Media Check List

- Business purpose; communication style; industry
- Social media on company time
- Appropriate discussion of business activities
- Content- confidentiality, copyright
- Purpose – personal, business use
- Job descriptions
- Auditing and investigation
- Consequences
- Training

Social Media

- Your best defense is _ _ _ t o _ _ i t
- 2nd best defense is to write clear and effective policies and procedures

Recent Examples

- St. Mary’s Medical Center – Long Beach, CA
  - Nurses and other staff take photos of a stabbing victim and post them on Facebook
- Tri-City Medical Center – Long Beach, CA
  - No patient names or other identifiers used but there was a discussion on Facebook about patients

Recent Examples

- Mercy Walworth Medical Center – Lake Geneva, WI
  - Photos taken of patient x-ray and posted to Facebook.
- Oakwood Hospital and Medical Center – Dearborn, MI
  - Employee posted information about a patient who she alleged was a “cop killer”.

Recent Examples

- Providence Holy Cross Medical Center – Mission Hills, CA
  - Contract employee posted a photo of the patient’s medical record to poke fun at a patient.
  - Photo included the patient’s name and the date she was admitted
  - Also included comments about the patient’s medical condition

Recent Examples

- When others pointed the privacy violation the poster’s response was “People, it’s just Facebook. Not reality. Hello? Again . . .it’s just a name out of millions and millions of names. If some people can’t appreciate my humor then tough. And if you don’t like it, too bad, because it’s my wall and I’ll post what I want to.”

Organizational Culture

Discussion

Organizational Culture

- Knowledgeable workforce
  - responsibilities (roles)
  - relevance (why factor)
    - regulations/standards
    - golden rule
  - controls environment (people and technology)
  - procedures
  - ongoing education and orientation

Organizational Culture

- Why factors
  - HIPAA and HITECH
  - **Medicare**
  - **Health Care Reform Act**
  - State Laws
  - Accreditation

Organizational Culture

- 42 C.F.R. § 482.24 CMS conditions of participation - Patient rights, requires hospitals to assure that:
  - Patient records are confidential;
  - Unauthorized persons cannot gain access to or alter patient records; and
  - Patient records are released only to authorized persons in accordance with law.
- Health Care Reform
  - Information exchange (EHR)
  - Meaningful use and data driven

Organizational Culture

- Be the influence and get the message out
  - Create partnerships
  - Communicate through committees
  - Develop and make resources and tools accessible and available
  - Be available to attend meetings and provide live education
  - Contribute to internal communications
    - Magazines/journals

Resources and Tools

- DHHS - Office of Civil Rights
  - http://www.hhs.gov/ocr/privacy/index.html
- HCCA net HIPAA Forum
  - http://community.hcca-info.org/HCCA/Communities/DiscussionGroups/ViewThread/?GroupId=121&MessageKey=7e65ddcc-fc96-4b21-ad5b-de231573b279
- CMS Conditions of Participation
  - https://www.cms.gov/CFCsAndCoPs/
- HITECH Answers – Free whitepapers
  - http://www.hitechanswers.net/ehr-incentive-program/hipaa-and-security-compliance/