



OCR Privacy and Security Update

**4th National HIPAA West Summit
October 4-6, 2010**

**Adam Greene, JD, MPH
Senior Health IT and Privacy Specialist**



Agenda

- Recent OCR Activities
- Key Areas of HITECH NPRM
- Breach Notification Statistics
- Upcoming OCR Activities





Recent OCR Activities

- Breach Notification Interim Final Rule and Unsecured PHI Guidance (Aug. 2009)
- GINA Proposed Rule (Oct. 2009)
- HITECH Enforcement Interim Final Rule (Oct. 2009)
- Workshop on De-identification (March 2010)
- Risk Analysis Guidance (July 2010)
- HITECH Proposed Rule (July 2010)



HITECH NPRM

- Business associates
 - Direct liability
 - Subcontractors
 - Clarification of HIOs, E-Prescribing Gateways, PHRs
- Enforcement
 - Willful neglect
 - Definition of reasonable cause



HITECH NPRM

- Marketing
- Fundraising
- Sale of PHI
- Right to request restrictions
- Minimum necessary (request for comments)



HITECH NPRM

- Notice of privacy practices
- Research authorizations
- Student immunization records
- Decedent information
 - Limit protections to 50 years
 - Clarify communications with friends and family
- Electronic access



Breach Notification Statistics

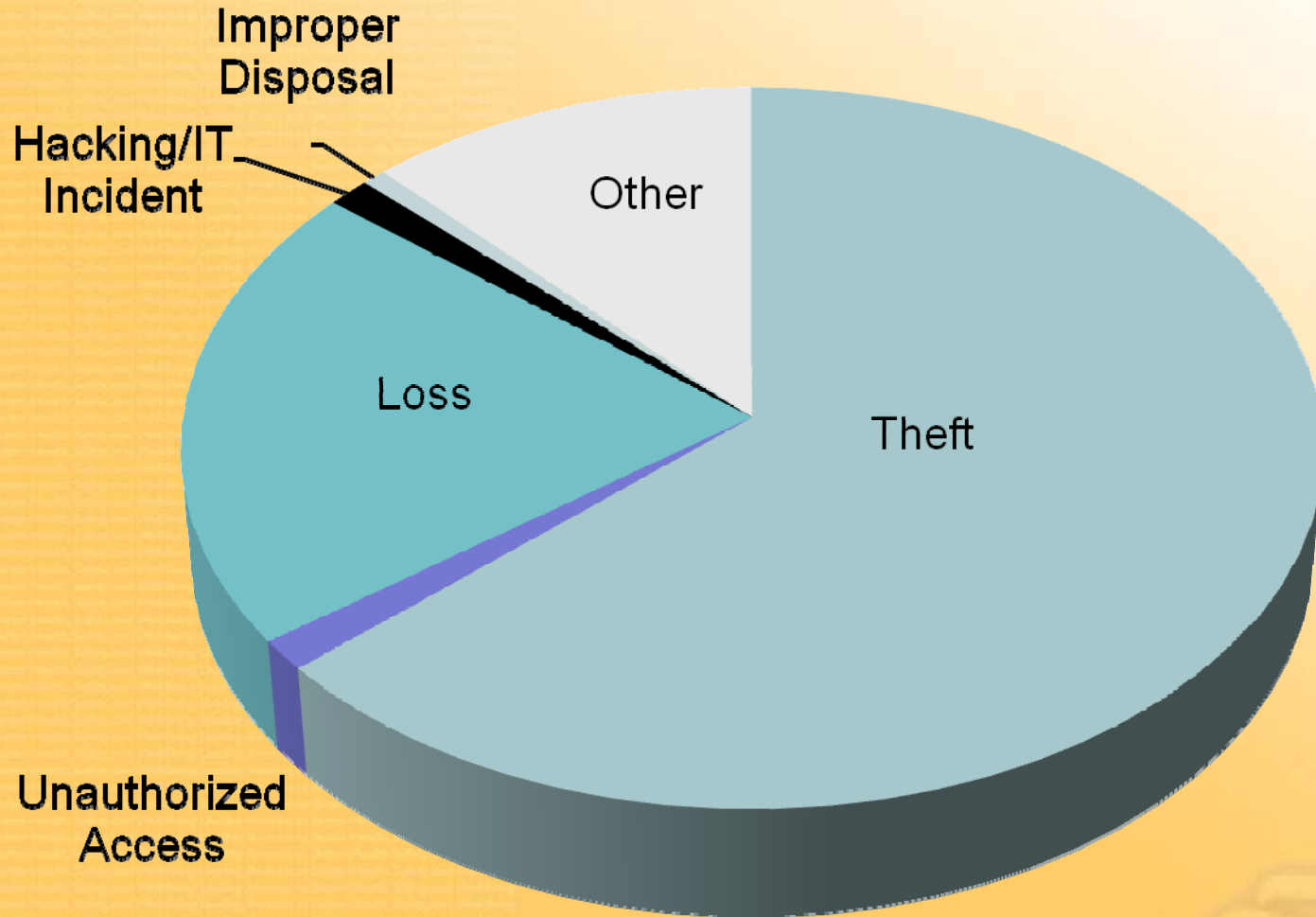
(as of September 14, 2010)

- 160 reports involving over 500 individuals
- Over 8,500 reports involving under 500 individuals
- Top causes of large breaches
 - Theft
 - Unauthorized Access
 - Loss
- Top media types for large breaches
 - Laptops
 - Paper records
 - Desktop Computers
 - Portable electronic devices



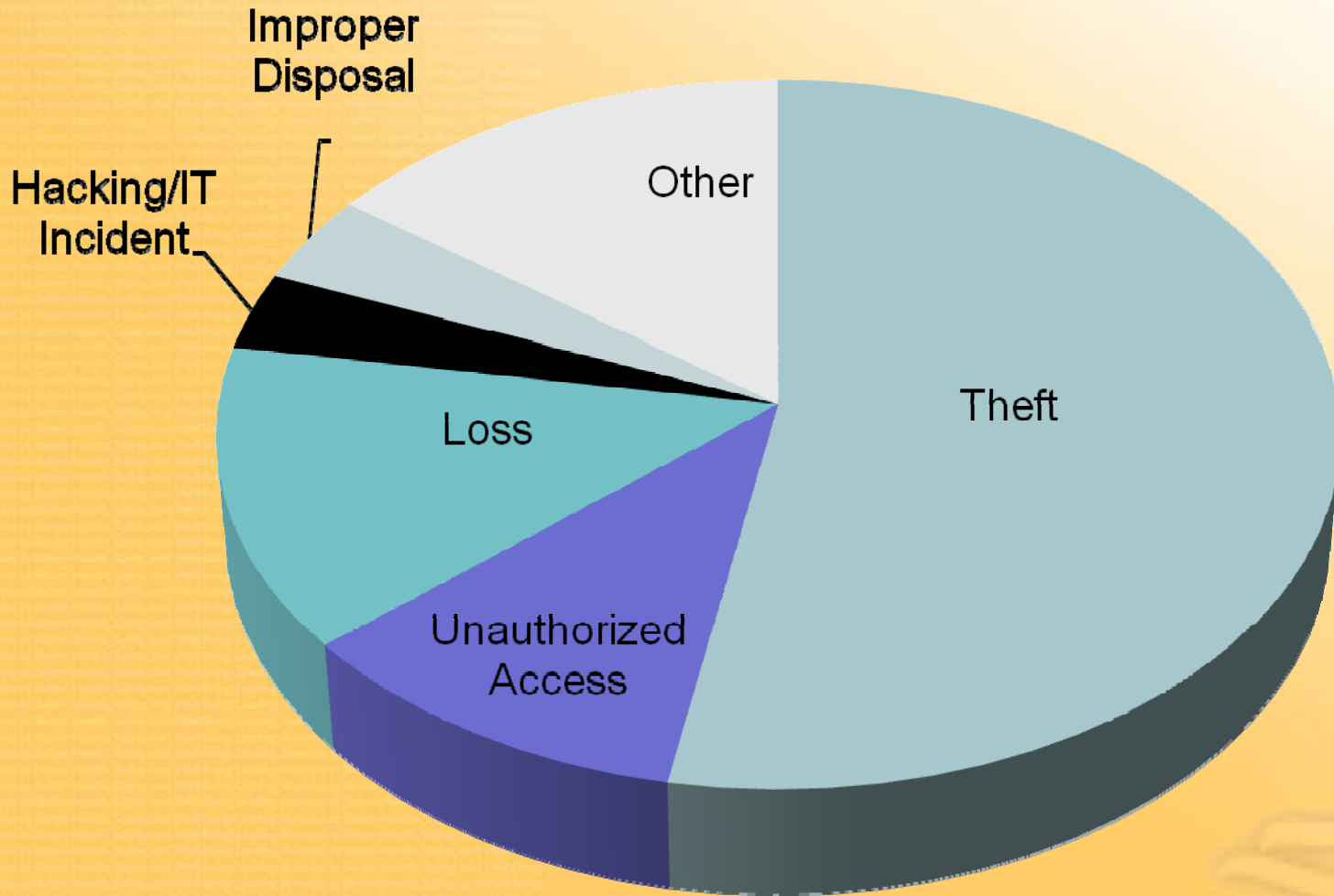
Breach Notification:

Type of 500+ Breach (by affected individuals)





Breach Notification: Number of 500+ Breaches





Upcoming OCR Activities

- Accounting of Disclosures Rule
- Reports to Congress on Compliance, Breach Notification
- National Outreach Campaign
- HIPAA Audit Program
- State Attorneys General Training
- Privacy Rule Minimum Necessary Guidance
- De-identification Guidance
- Final Rules on HITECH, Breach Notification, Enforcement, and GINA



Upcoming OCR Activities

- Accounting of Disclosures Rule
 - Disclosures for treatment, payment, health care operations
 - Through an EHR
 - Balance interests of individuals and administrative burden on covered entities



Upcoming OCR Activities

- Report to Congress on Breach Notification
 - CY 2009
 - Information on large and small breaches
- Report to Congress on Enforcement
 - Aggregate and CY 2009 enforcement data



Upcoming OCR Activities

- National Outreach Campaign
 - Series of community discussions on Health IT and HIPAA
 - Improved consumer outreach materials
 - Improved website navigation





Upcoming OCR Activities

- **HIPAA Audit Program**
 - Addition to complaint and compliance review process
 - Reviewing effectiveness of various audit models
- **State Attorneys General Training**
 - Education on HIPAA
 - Coordination



Upcoming OCR Activities

- **Minimum Necessary Guidance**
 - Requested comments in NPRM
 - Sunsets limited data set language of HITECH Act
- **De-identification Guidance**
 - Convened workshop
 - Clarify how to assure that PHI is de-identified



Upcoming OCR Activities

- Final regulations
 - Breach notification
 - HITECH modifications
 - Enforcement
 - GINA
 - Accounting of disclosures
- Coordinated to synchronize changes



Want more information?

The OCR website:

<http://www.hhs.gov/ocr/privacy/>

My contact:

adam.greene@hhs.gov

