United States Department of Health & Human Services
Office of the Secretary
Office for Civil Rights (OCR)

Breach Notification for HIPAA Covered Entities and Business Associates

NIST/OCR HIPAA Security Conference

June 7, 2012

David Holtzman, JD, CIPP/US/G
Health Information Privacy & Security Division

Breach Notification
45 CFR 164 Subpart D

- HHS Issued RFI & Guidance – April 2009
  - Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
  - 74 Federal Register 19006 (April 27, 2009)
- HHS Issued IFR – August 2009
  - Effective for breaches after 9/23/09
  - 74 Federal Register 42740 (August 24, 2009)

Breach Notification IFR

- Covered entities and business associates must provide notification of breaches of ***unsecured*** protected health information

- HHS Breach Notification Guidance: PHI is "unsecured" if it is NOT
  - Encrypted
  - Destroyed

What is a Breach

- Impermissible use/disclosure which "compromises privacy/security" of PHI
  - Poses a significant risk of harm
    - Financial
    - Reputational
    - Other harm
- Determined through risk assessment

Exceptions for Harmless Error

- Exceptions for inadvertent, harmless mistakes
  - Unintentional access by workforce member and no further impermissible use or disclosure
  - Inadvertent disclosure at same CE/BA/OHCA and no further impermissible use or disclosure
  - Recipient could not reasonably have retained the PHI

Breach Notification Requirements

- Covered entity must notify each affected individual of breach
- Business associate must notify covered entity of breach
- Notification to HHS and media in breaches affecting >500 individuals
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach

OCR Compliance Reviews

- OCR opens a review of all breach reports involving >500
- CE should be prepared to respond with:
  - Determination of the root cause of disclosure
  - Identifying gaps in compliance with Privacy and Security Rules that led to the breach
  - Provide evidence that the root cause has been addressed to insure that further breaches do not occur

Breach Notification Highlights

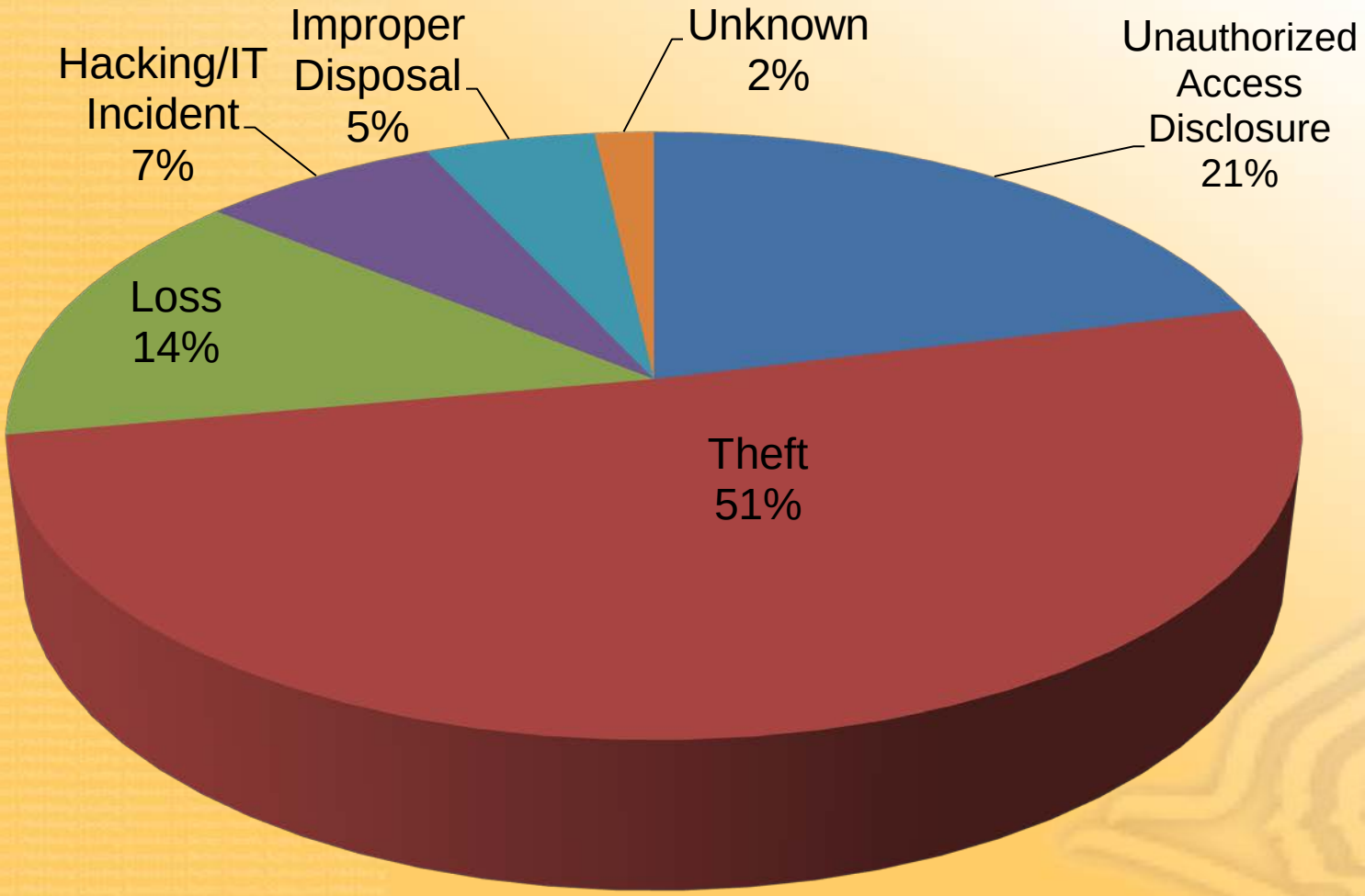
September 2009 through May 10, 2012

- 435 reports involving a breach of over 500 individuals
  - Over 20 million individuals affected
  - Theft and loss are 65% of large breaches (about 70% of these incidents involved ePHI)
  - Laptops and other portable storage devices account for 38% of large breaches
  - Paper records are 24% of large breaches
- 57,000+ reports of breaches of under 500 individuals

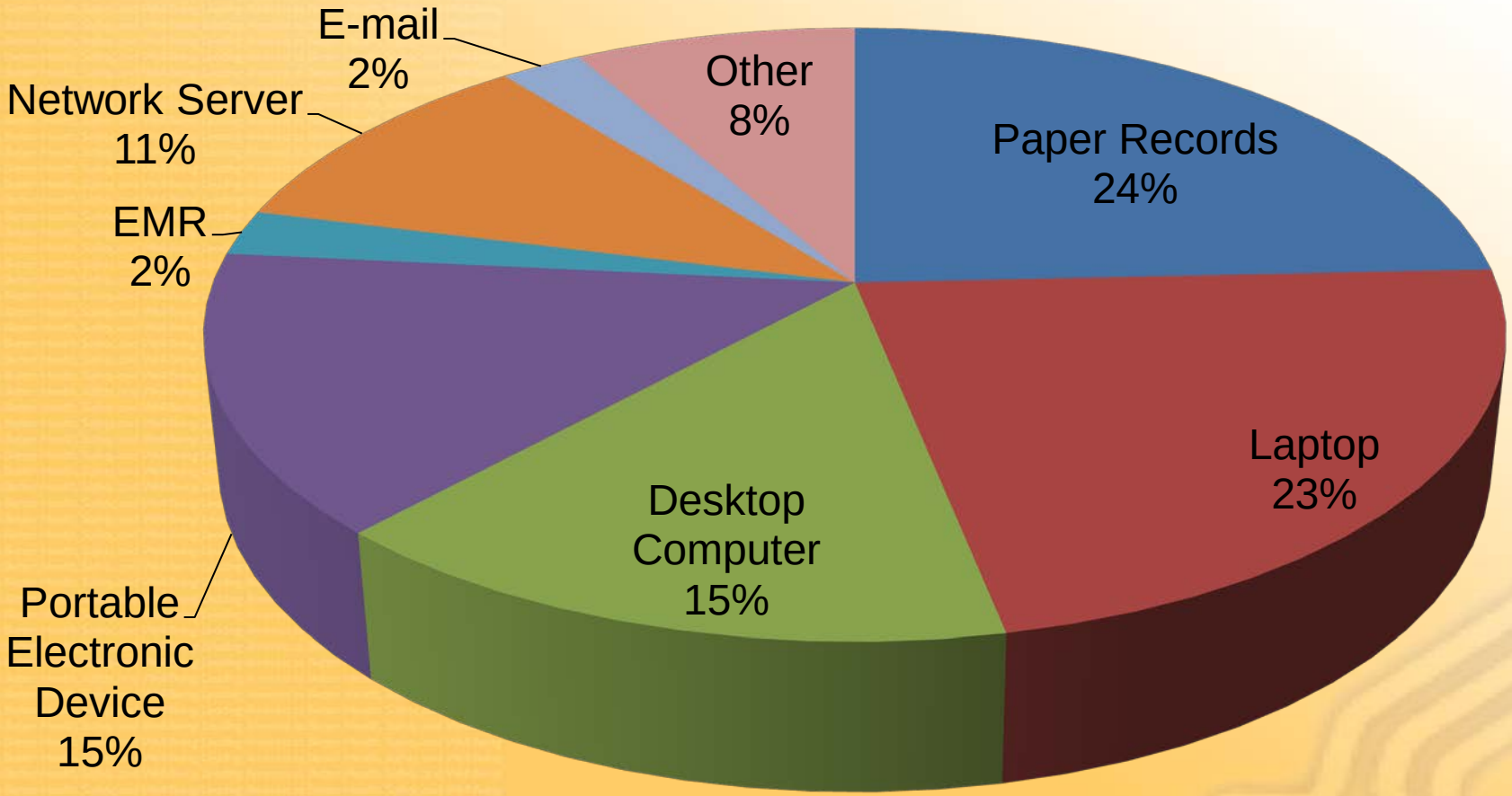
Breaches by Business Associates

- Number and impact of breaches by business associates indicate significant failures in safeguarding PHI
- Business associates responsible for 22% of breaches involving >500 individuals
- Breaches caused by business associates have affected 60% of all individuals whose PHI disclosed in a breach incident

Breach Notification:
500+ Breaches by Type of Breach



Breach Notification:
500+ Breaches by Location of Breach



Want More Information?

- The OCR website is:
  http://www.hhs.gov/ocr/privacy/

- My contact is:
  david.holtzman@hhs.gov