United States Department of
Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA Security Rule and HITECH Breach Notification Trends in Enforcement Activity

Nineteenth HIPAA Summit
March 9, 2011

David S. Holtzman, JD
Office for Civil Rights
Health Information Privacy Division

Topics

- How OCR Enforces the HIPAA Security Rule
- HIPAA Security Rule Enforcement Recap
- HITECH Breach Notification Recap
- Some Lessons Learned

United States Department of
Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

How OCR Enforces the HIPAA Security Rule

Complaints Alleging a Violation

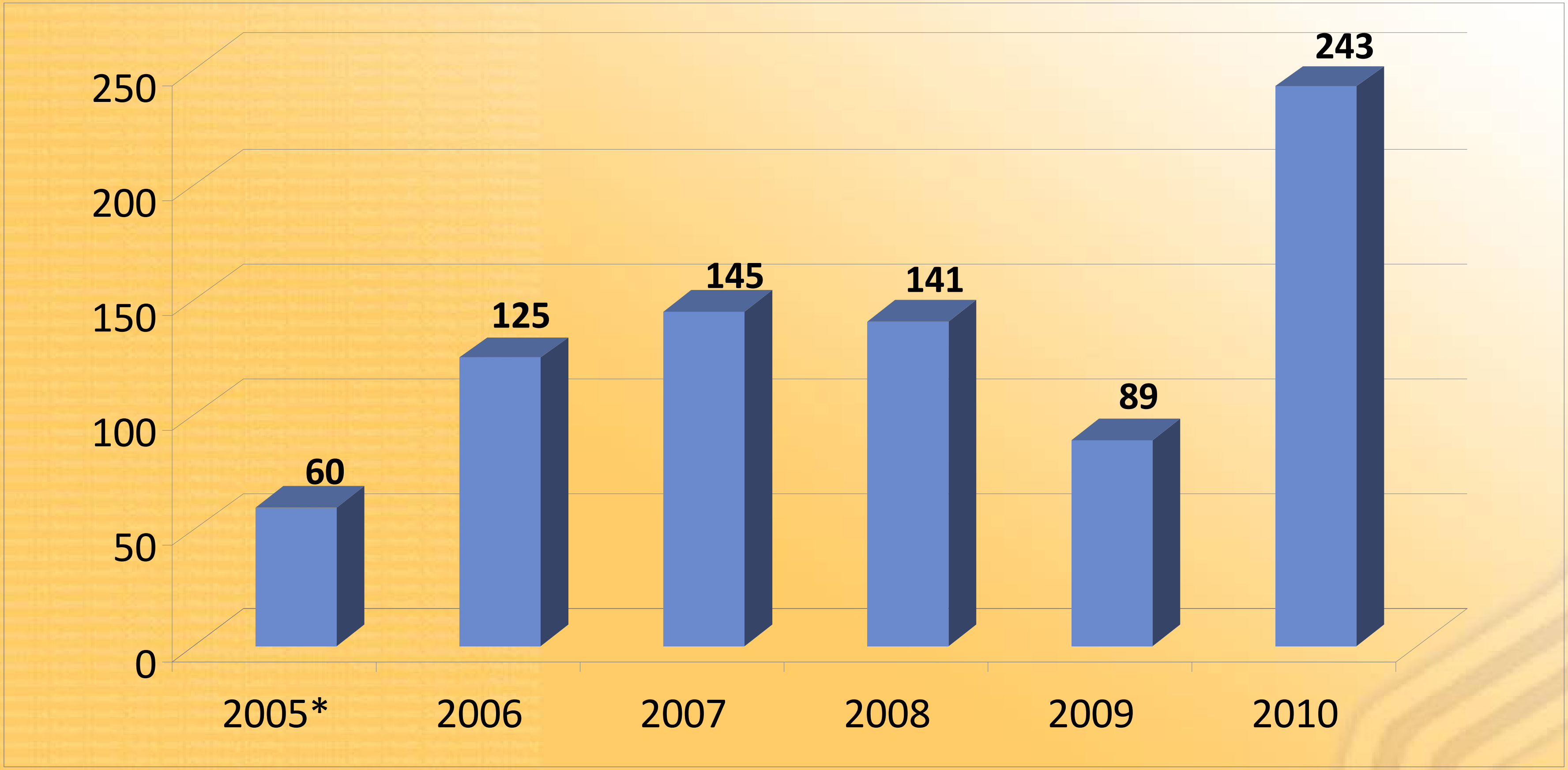
- Every complaint received by OCR is reviewed & analyzed
- An investigation is launched if the facts and circumstances alleged indicate a failure to comply
- Complaints that allege violations under more than one of OCR's authorities (e.g., privacy, security, or breach notification rules) will be investigated as a single case

Compliance Reviews

- Reviews policies and procedures of a covered entity to determine compliance with the health information privacy rules
- OCR initiates when a media report or information from another agency reports a failure to safeguard PHI or other indication of noncompliance with the HIP rules
- OCR initiates a review in all breach reports of >500 made to HHS

HIPAA Security Rule Enforcement Activity

Security Complaints & Reviews Opened



* Partial Year

Security Rule delegated to OCR July 27, 2009

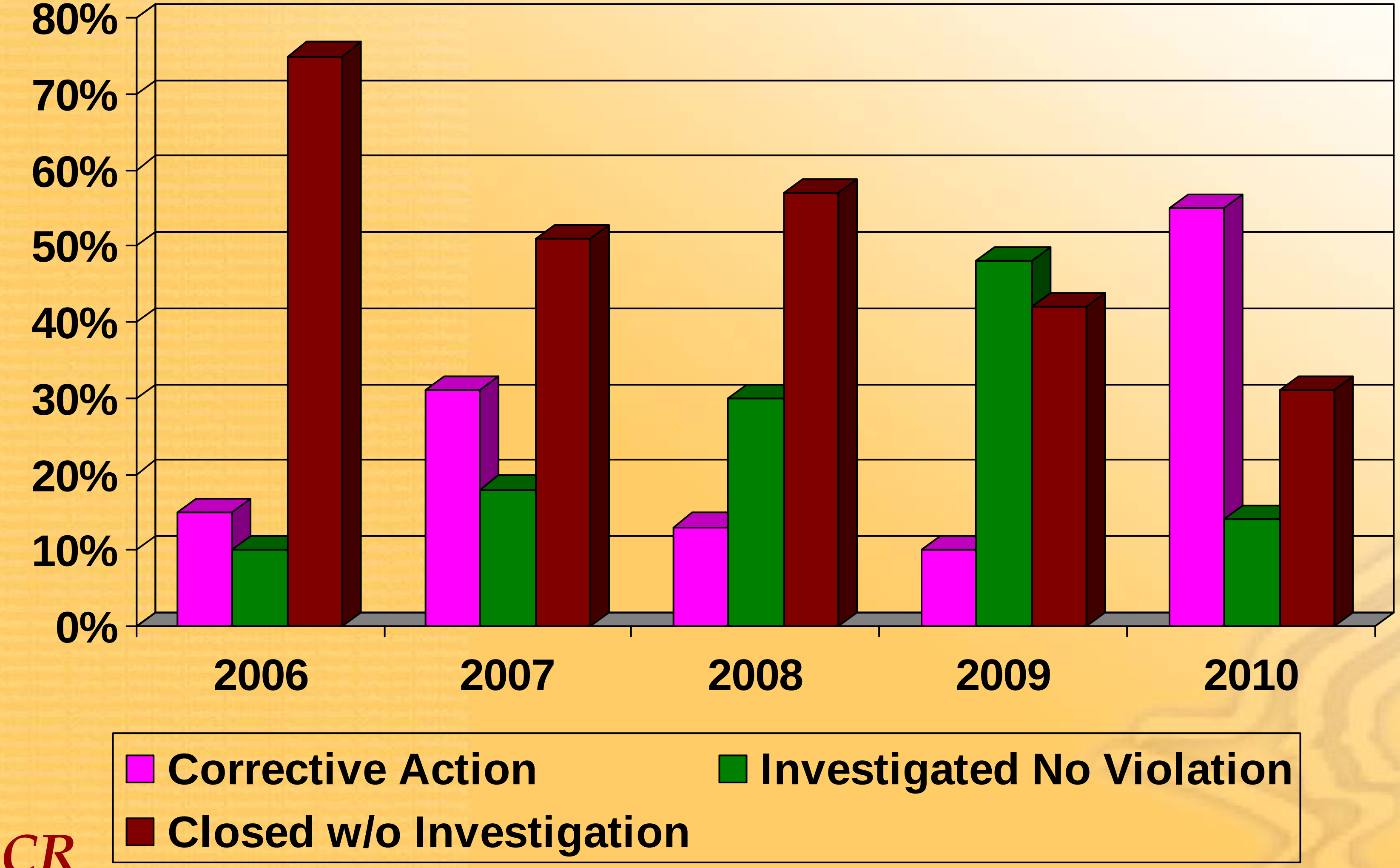
OCR

Security Complaints & Reviews Resolved

	2005	2006	2007	2008	2009	2010	TOTAL
Corrective Action	**0**	**9**	**41**	**21**	**9**	**70**	**150**
Investigated and No Violation Found	**0**	**6**	**24**	**50**	**41**	**18**	**139**
Closed Without Investigation	**7**	**44**	**68**	**93**	**36**	**40**	**287**
TOTAL:	***7***	***59***	***133***	***164***	***86***	***128***	***577***

Security Rule delegated to OCR July 27, 2009

Security Closures by Type



OCR

Most Frequent Security Rule Issues

Standard or Specification	Type of Safeguard	Count
Response and Reporting (R) §164.308(a)(6)(ii)	Administrative	179
Awareness & Training §164.308(a)(5)(i)	Administrative	144
Access Control §164.312(a)(1)	Technical	141
Information Access Management §164.308(a)(4)(i)	Administrative	126
Workstation Security §164.310(c)	Physical	84

United States Department of
Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HITECH Breach Notification Rule Reports and Trends

Breach Notification Highlights

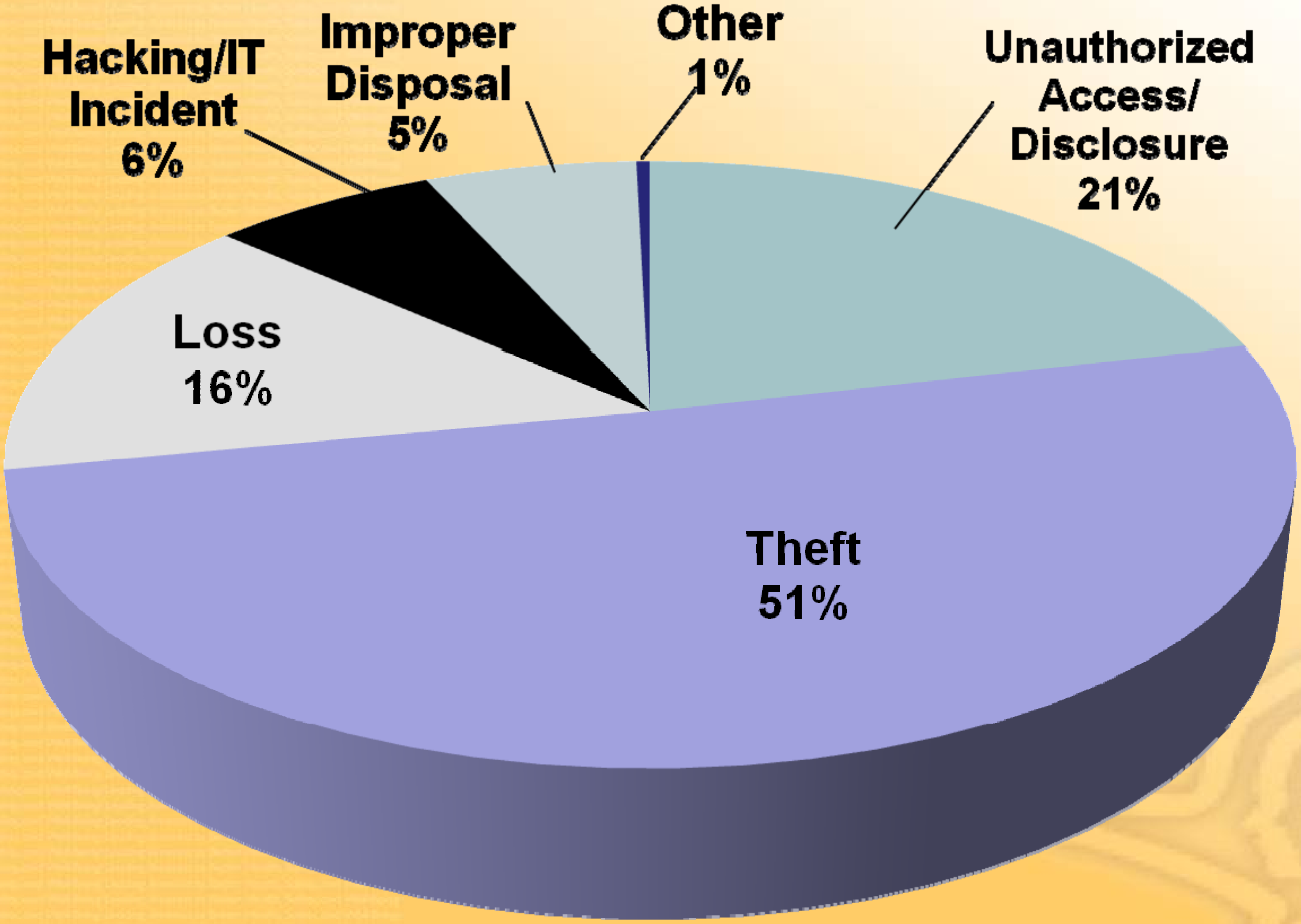
September 2009 through December 2010

- 221 reports involving a breach of over 500 individuals
  - Theft and Loss are 67% of large breaches
  - Laptops and other portable storage devices account for 38% of large breaches
  - Paper records are 21% of large breaches

- 14,000+ reports of breaches of under 500 individuals

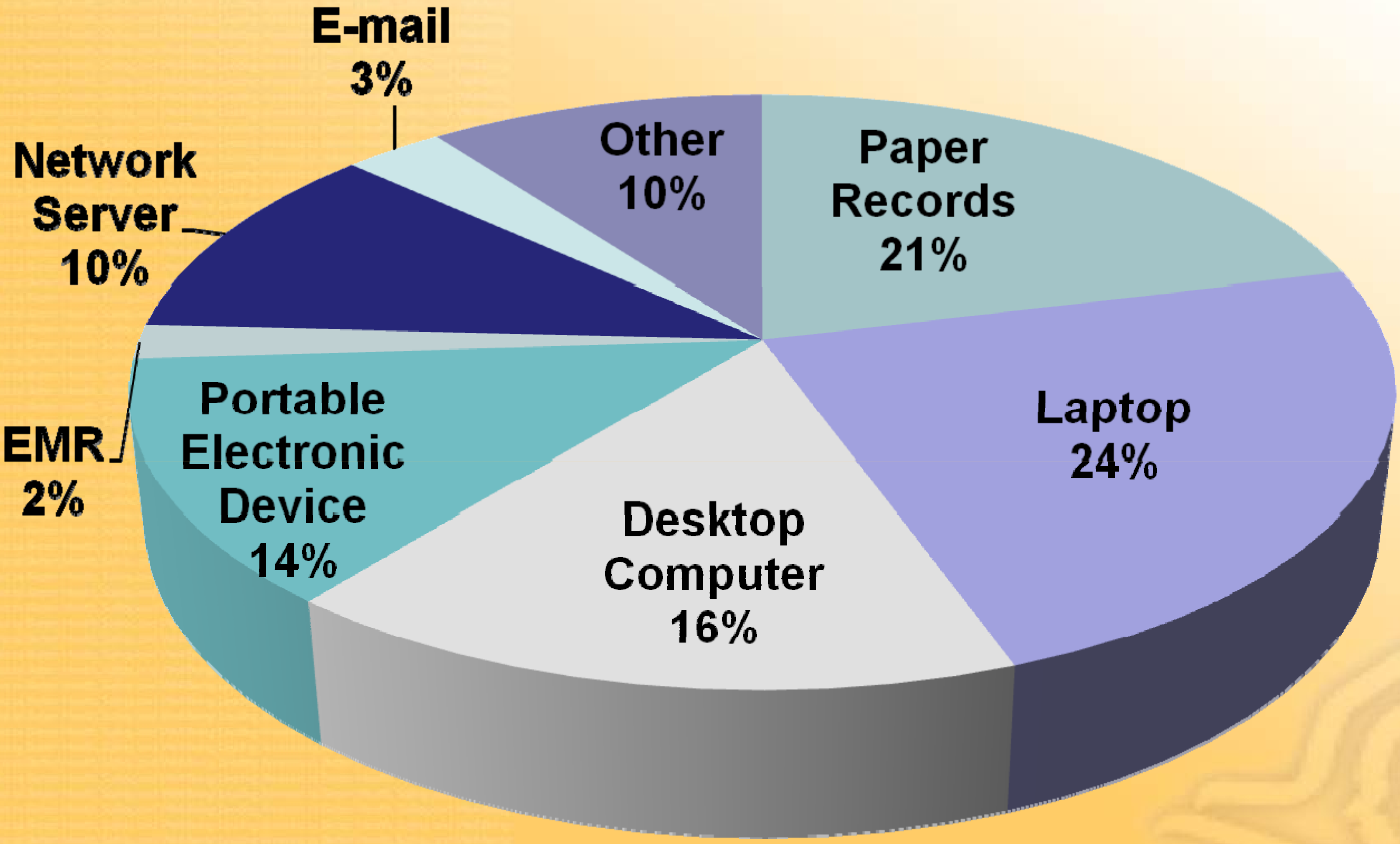
Breach Notification:

500+ Breaches by Type of Breach



Breach Notification:

500+ Breaches by Location of Breach



OCR

Lessons Learned

- Reduce risk through network or enterprise storage as alternative to local devices
- Encryption of data at rest on any desktop or portable device/media storing EPHI
- Clear and well documented administrative and physical safeguards on the storage devices and media which handle EPHI
- Raise the security awareness of workforce members to promote good data stewardship

Want More Information?

The OCR website, http://www.hhs.gov/ocr/privacy/ offers a wide range of helpful information about health information privacy including educational information, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules.