



Keynote Address

23rd National HIPAA Summit

Director Jocelyn Samuels
HHS Office for Civil Rights
March 16, 2015



Breach Highlights

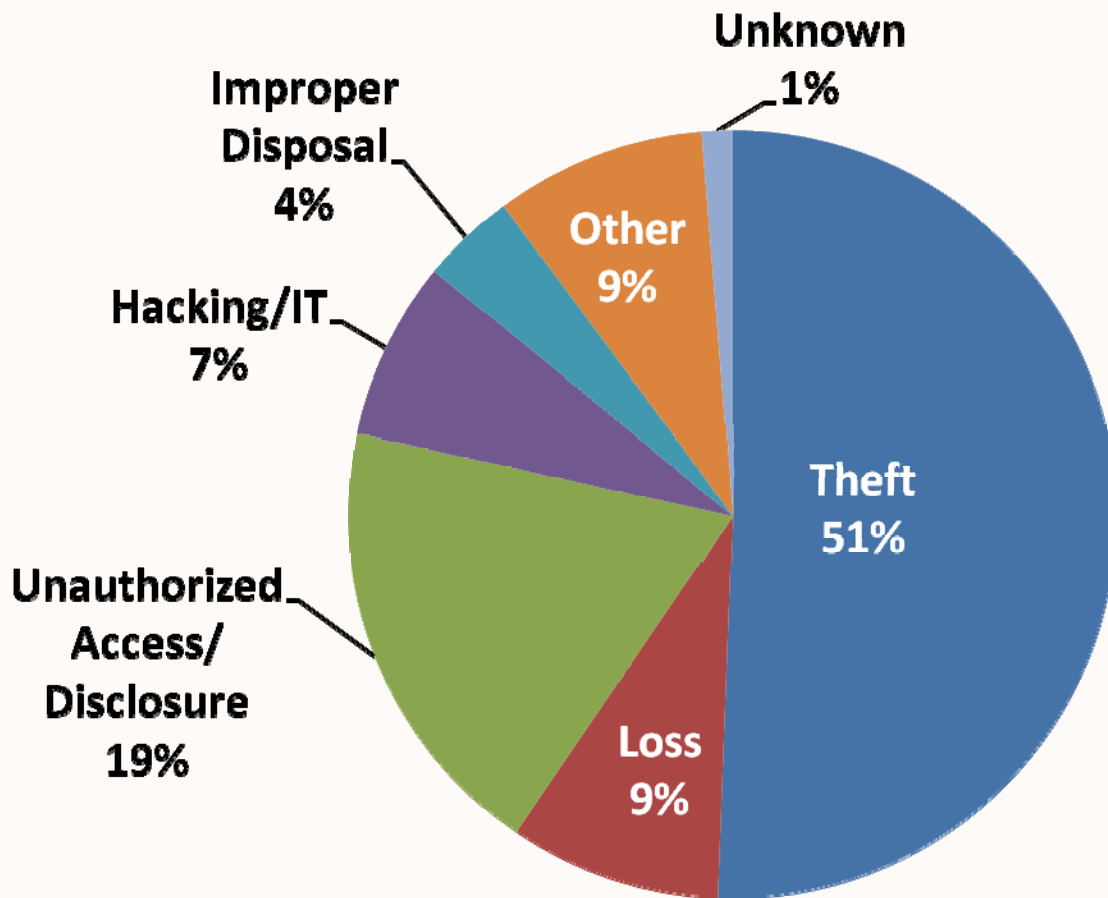


September 2009 through February 27, 2015

- Approximately 1,144 reports involving a breach of PHI affecting 500 or more individuals
 - Theft and Loss are 60% of large breaches
 - Laptops and other portable storage devices account for 32% of large breaches
 - Paper records are 22% of large breaches
- Approximately 157,000+ reports of breaches of PHI affecting less than 500 individuals

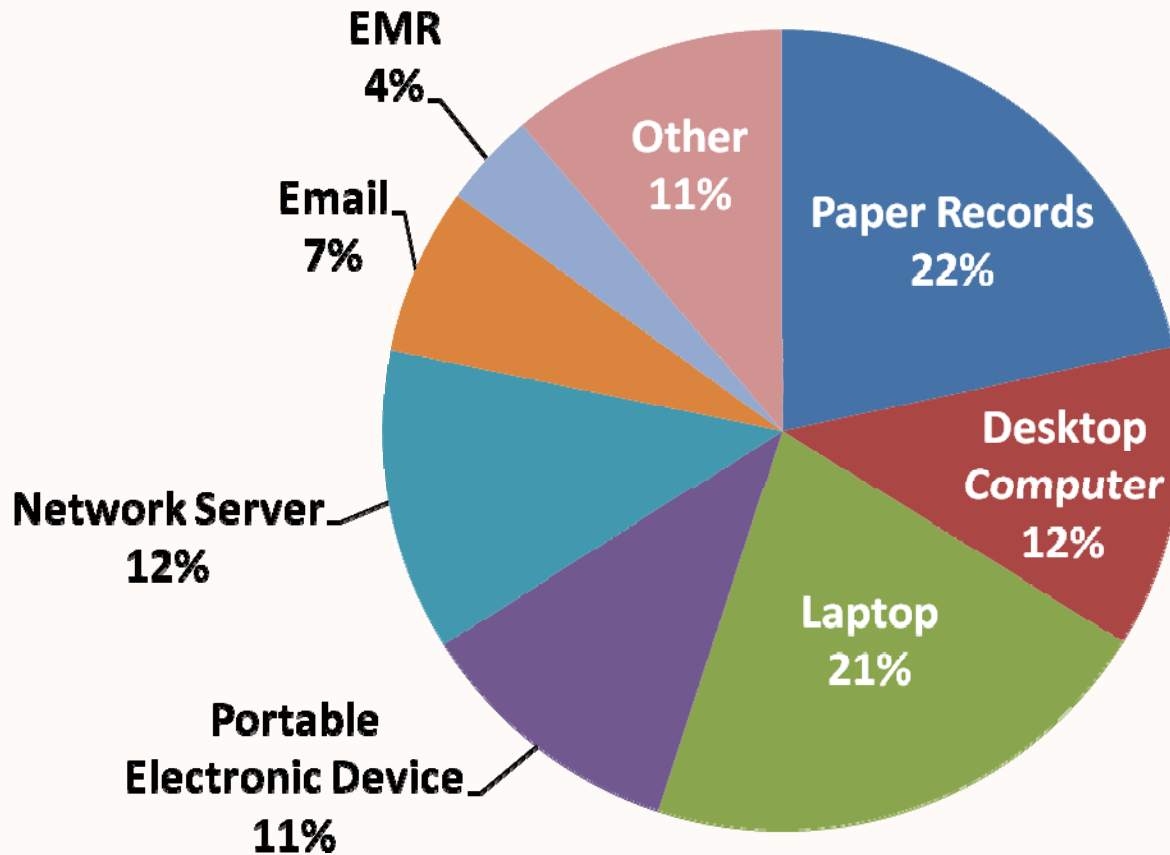


500+ Breaches by Type of Breach as of 2/2015





500+ Breaches by Location of Breach as of 2/2015





Enforcement Highlights



Complaints and Compliance Reviews

- Over 110,000 complaints received to date
- About 1,200 compliance reviews initiated
- Over 30,000 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints this year
- Launched Customer Response Center (CRC) and Central Intake Unit (CIU) for greater efficiency and responsiveness





Resolution Agreements/Corrective Action Plans and Civil Money Penalties

- 23 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 1 civil money penalty



Anchorage Community Mental Health Services (December 2014)

- Breach affecting 2,743 individuals due to malware compromising the security of its information technology resources
- \$150,000 settlement and corrective action plan to correct deficiencies, including reporting to OCR for a two-year period



Parkview Health System Settlement (June 2014)

- Over 5,000 medical records were left unattended in a public area
- Corrective action plan requiring review of policies and procedures for safeguarding PHI and \$800,000 settlement amount



NYP and CU Settlements (May 2014)

- ePHI of 6,800 patients accessible on internet search engines
- Entities failed to make efforts prior to breach to assure information was secure
- Corrective action plans and \$4,800,000 settlement amount



- Risk analysis & risk management
- Security and control of portable electronic devices
- Proper disposal/transfer
- Physical access controls
- Training



Policy Updates



National Instant Criminal Background Check (NICS) Rulemaking

- January 2013 – one of 23 executive actions to reduce gun violence
- April 2013 – Advance Notice of Proposed Rulemaking (ANPRM) on need for HIPAA rule change for NICS reporting
- January 2014 – NPRM published
 - Express disclosure permission in Privacy Rule for designated NICS reporters or entities making mental health commitment or adjudication decisions
 - Limited to identity, demographics; not clinical data or medical records
- March 10, 2014 – comment period closed
- Final Rule at OMB



Clinical Laboratory Improvement Amendments (CLIA) Final Rule

- Joint Rulemaking
- Centers for Medicare and Medicaid Services (CMS) – Amends CLIA regulations to allow labs to give patients access to completed test results
- OCR – Amends HIPAA right to access to remove exemption for CLIA labs
 - Individual has right to get copy of test reports directly from labs
 - Access obligations on labs same as for other CEs
 - Individual can still go through physician to obtain test results
- Dates
 - Published February 6, 2014; effective April 7, 2014; compliance required By October 6, 2014



HIPAA Privacy Rule and Sharing Information Related to Mental Health

- Provides guidance on when it is appropriate under the Privacy Rule to share the PHI of a patient who is being treated for a mental health condition
- Clarifies circumstances when health care providers are permitted to communicate with friends, family members, law enforcement, or others



Understanding *Spouse, Family Member, and Marriage*

- Addresses effect of 2013 Supreme Court Windsor decision on certain provisions
 - Permitted disclosures to family members
 - Prohibited uses & disclosures of genetic information for underwriting
- Clarifies that spouses include both same-sex and opposite-sex individuals who are legally married, whether or not they live or receive services in a jurisdiction that recognizes their marriage



Guidance on HIPAA Privacy in Emergency Situations

Issued during the Ebola outbreak:

- To remind HIPAA covered entities and their business associates of the ways in which PHI may be shared in an emergency situation
- To underscore that the protections of the Privacy Rule are not set aside during an emergency



Policy Development

- NICS Final Rule
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any CMP or monetary settlement collected
- More guidance, including cloud computing
- Collaboration with ONC on emerging technologies and new delivery systems



Outreach and Stakeholder Engagement Update



- Continued stakeholder engagement
 - Development of portal to enable stakeholders to effectively communicate with us about issues on which they would like additional guidance
- Website redesign for better navigation and usability



Audit



HITECH Audit Program

- Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
- Phase I completed
 - 115 pilot audits
 - Evaluation
- Phase II under development



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

Join us on Twitter @hhsocr