United States Department of Health & Human Services

Office for Civil Rights

Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

Marissa Gordon-Nguyen
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

June 2016

Updates

- Policy Development
- Breaches
- Enforcement
- Audit

POLICY DEVELOPMENT

Privacy and Trust Framework for PMI

- To guide the development and design of the PMI cohort
  - Final principles released November 2015
- Review of existing laws to address policy gaps or other issues
- Individual access at core of initiative

Data Security Policies and Framework

- To guide decision-making by organizations conducting or participating in precision medicine activities
  - Final principles released May 2016
- Builds on NIST Cybersecurity Framework
- Designed to be adaptable and responsive to the needs of multiple participating PMI groups

HIPAA Right of Access Guidance

- Issued in two phases in early 2016
  - Comprehensive Fact Sheet
  - Series of FAQs
- More to come

Access

- Scope: Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
- Form & Format & Manner: Individual has right to copy in form and format requested if "readily producible"
- Timeliness: Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner
- Limited Fees: Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
- Right to Direct a Copy to a 3rd Party: Individual has right to have entity transmit PHI to 3rd party of individual's choice (e.g., for research)

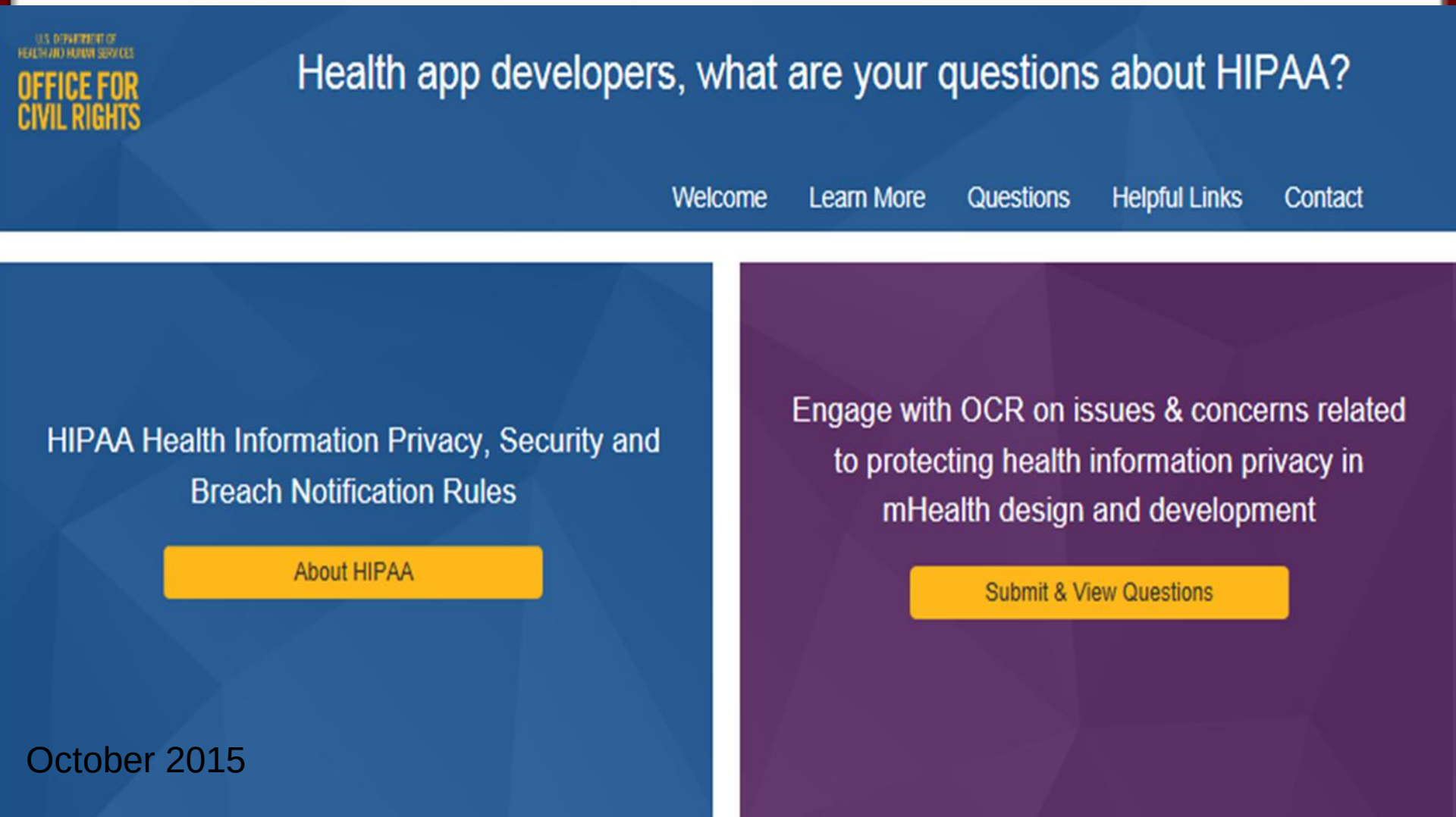
HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

United States Department of
Health & Human Services

Office for Civil Rights

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/



October 2015

Other Publications

- In collaboration with ONC, HIPAA Permitted Uses and Disclosures Fact Sheets issued in January 2016
- Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework issued in February 2016
- Infographic and educational videos on the individual right of access to protected health information issued June 2016

Policy Development – What's Coming

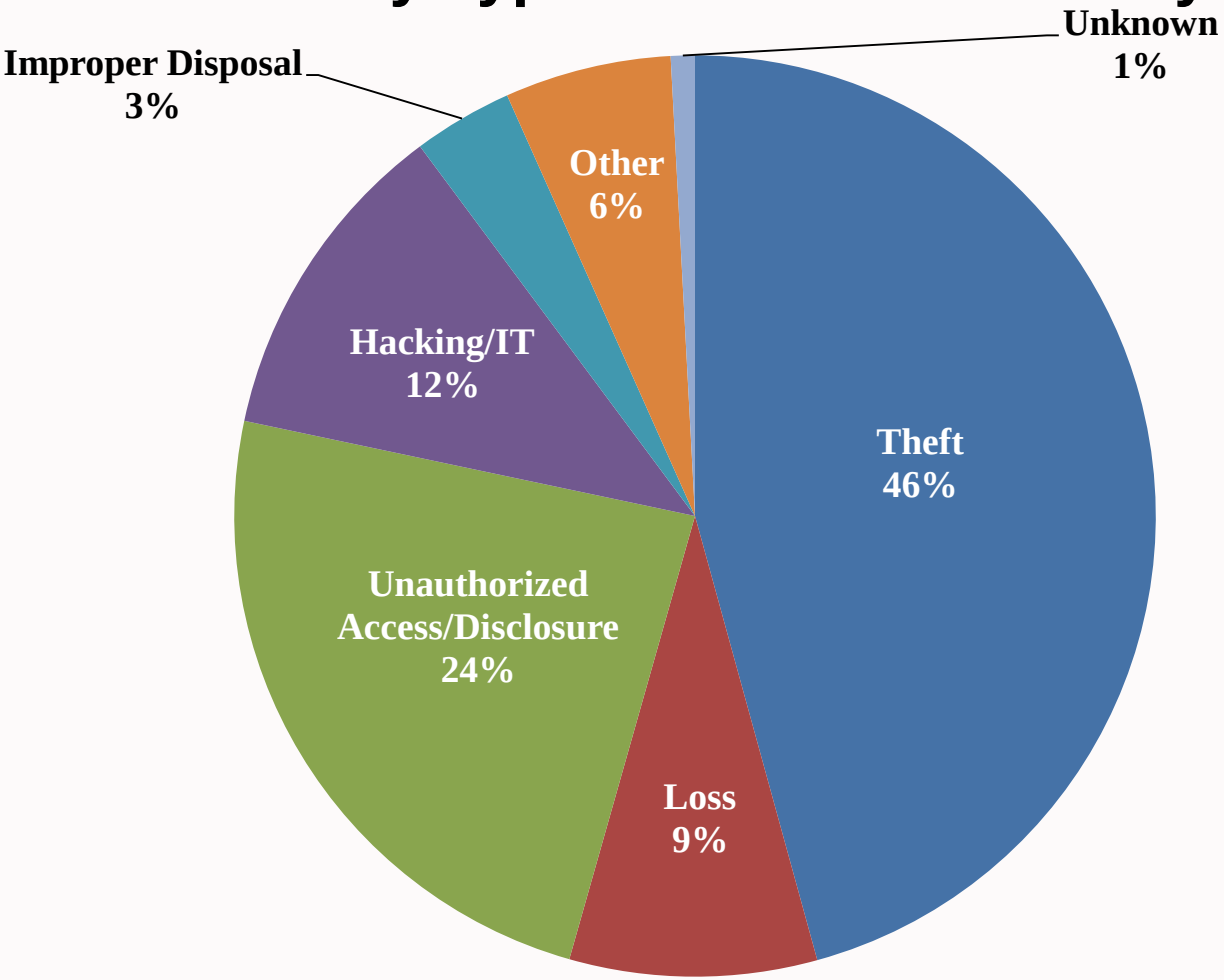
- Additional access guidance
- Guidance on ransomware
- Cloud guidance
- Guidance on text messaging
- Social media guidance
- PMI and research authorizations
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any CMP or monetary settlement collected

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

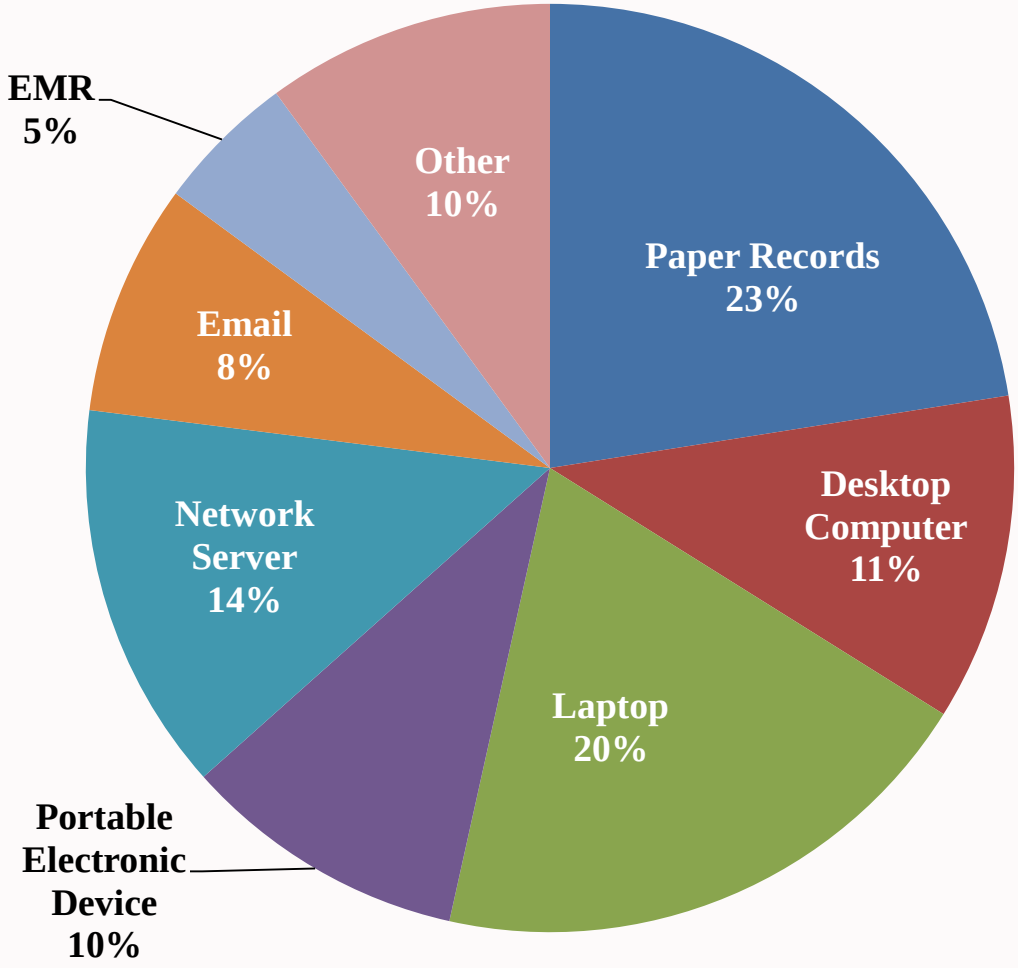
September 2009 through May 31, 2016

- Approximately 1,578 reports involving a breach of PHI affecting 500 or more individuals
  - Individuals affected are approximately 158,913,339
- Approximately 230,025 reports of breaches of PHI affecting fewer than 500 individuals

500+ Breaches by Type of Breach as of May 31, 2016



500+ Breaches by Location of Breach as of May 31, 2016



What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

General Enforcement Highlights

- Over 130,000 complaints received to date
- About 900 compliance reviews initiated
- Over 37,500 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints this year

As of 3/31/2016

General Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 34 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 2 civil money penalties

As of 4/30/2016

2016 Enforcement Actions

- New York Presbyterian Hospital
- Raleigh Orthopaedic Clinic
- Feinstein Institute for Medical Research
- North Memorial Health Care
- Complete P.T., Pool & Land Physical Therapy
- Lincare

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

AUDIT

HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open up compliance review (for example, if significant concerns are raised during an audit)
  - Also hope to learn from this next phase in structuring permanent audit program

Phase 1 (complete): Building Blocks, Pilot, Evaluation

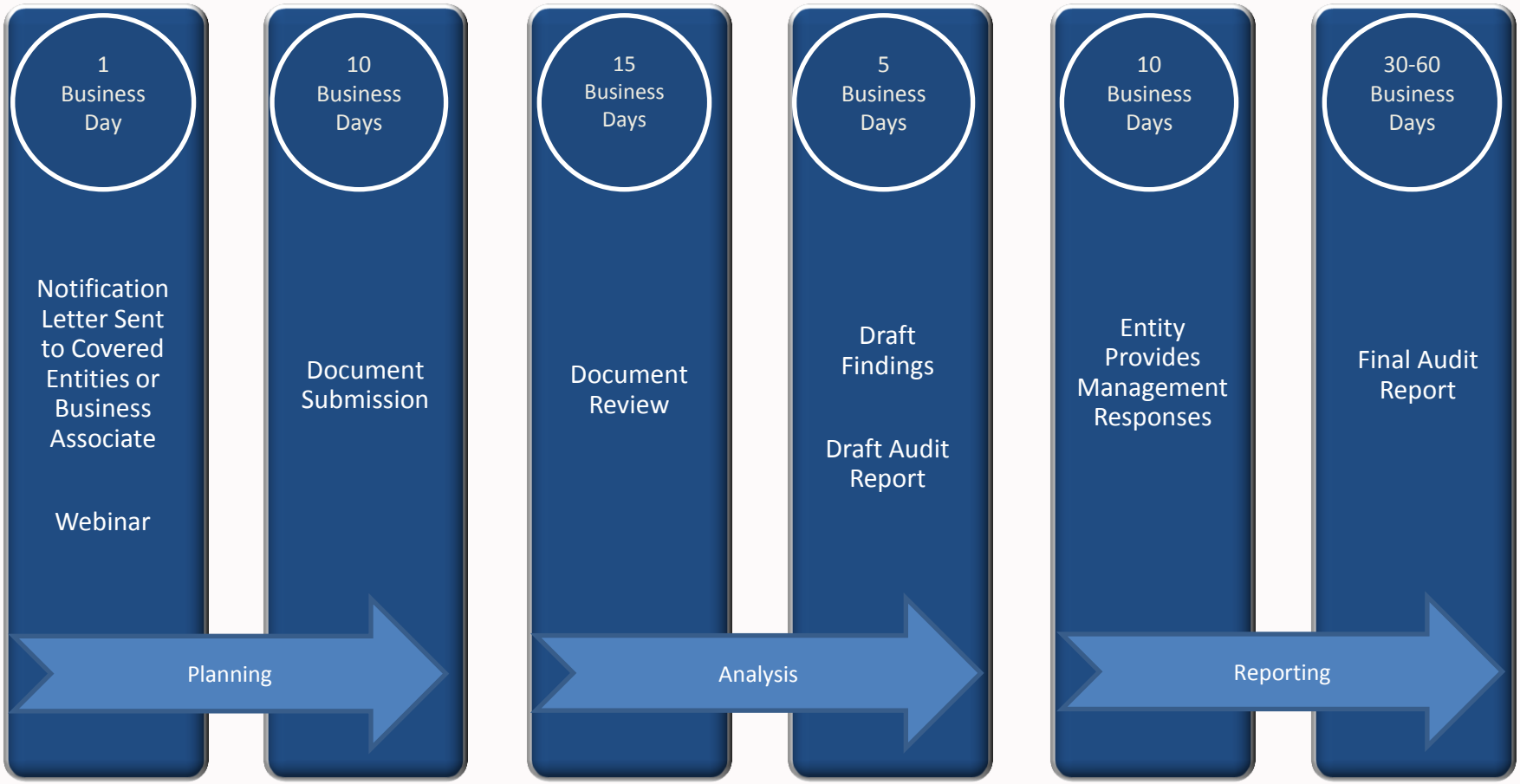
Phase 2 (in progress): Planning & Process

- Portal development
- Entity contact information verification
- Questionnaire to entity pool
- Entity selection
- Notification letter & document request
  - Business associates spreadsheet required

Questionnaire

- Information about the organization
  - Public or private
  - Single or multi-location
  - Part of or affiliated with another organization
- Type of covered entity or business associate
- Information on size of organization
  - # of beds
  - # of visits
  - # of members
  - Annual revenues
  - # of transactions
- Use of health information technology and ePHI

Desk Audit Process



Desk Audits

- For Covered Entities:
  - Security Rule: risk analysis and risk management
  - Breach Notification Rule: content and timeliness of notifications
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management
  - Breach Notification Rule: reporting to covered entity

More Information

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr

General Questions: OCRPrivacy@hhs.gov

Audit: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

Audit Mailbox: OSOCRAudit@hhs.gov