

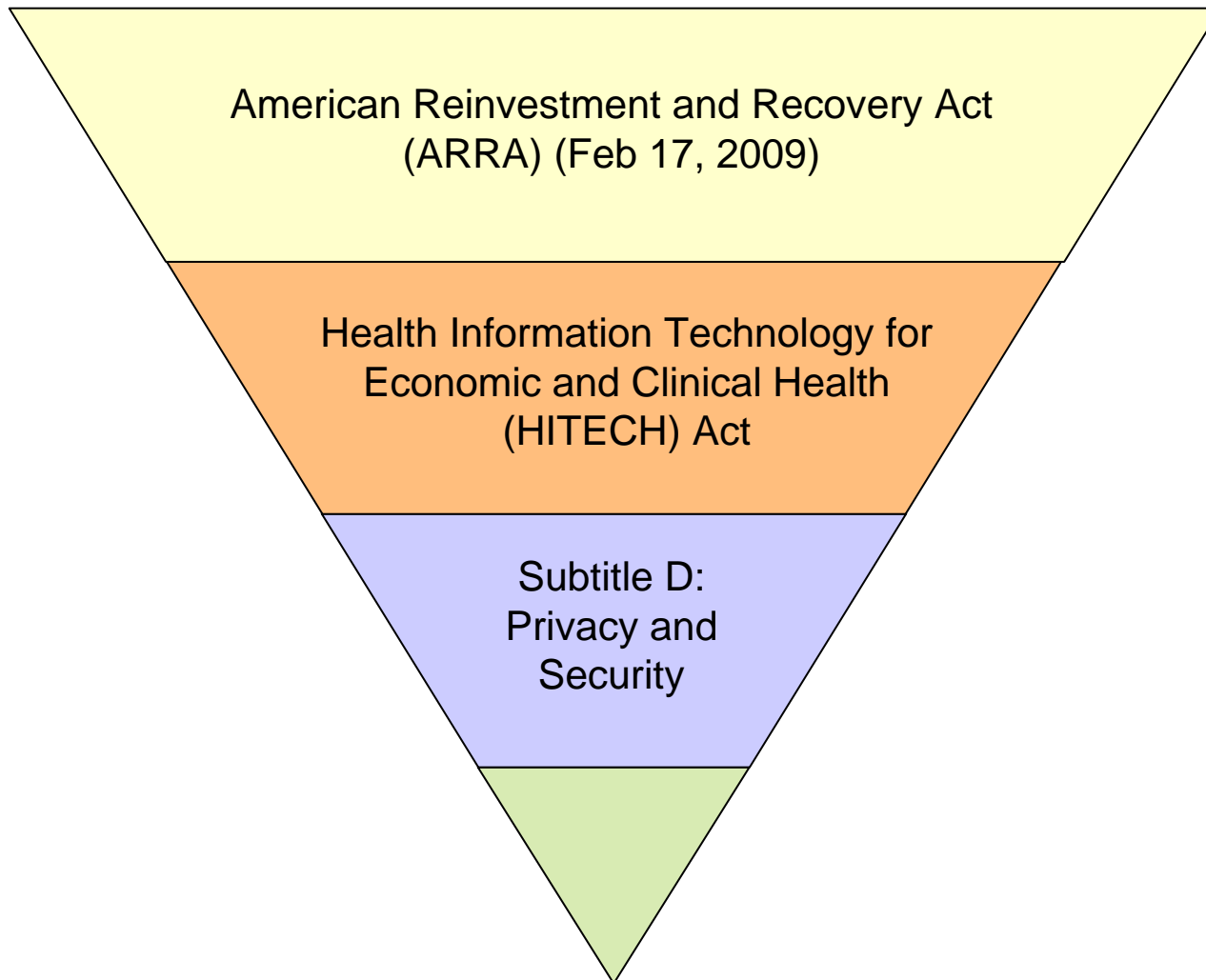


Discussion of the HITECH Privacy and Security Provisions

Presented by

Andy Reeder, Director, HIPAA Privacy and Security
Rush University Medical Center
Chicago, IL

Regulatory Context





Provisions of the ARRA

Tax Cuts and Credits

- Tax credits for individuals
- Alternative Minimum Tax
- Expanded Child Credit
- Expanded Earned Income Credit
- Homebuyer Credit
- Home Energy Credit
- Unemployment Benefits
- Bonus Depreciation
- Money Losing Companies
- Government Contractors
- Energy Production
- Taxes on Merged Banks
- Bonds
- Auto Sales

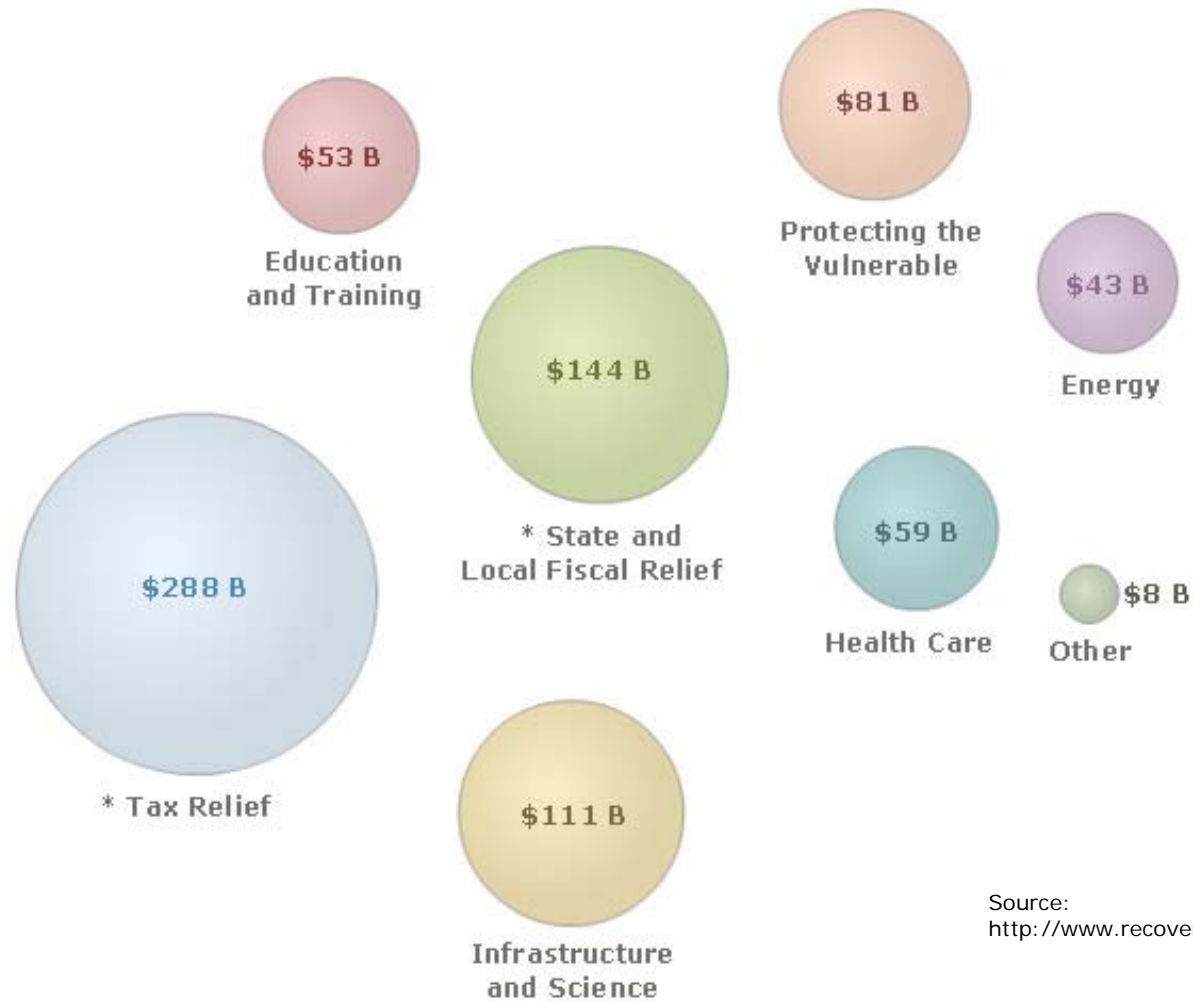


Provisions of the ARRA (cont.)

Spending

- Aid to low income workers and the unemployed
- Direct cash payments (Social Security)
- Infrastructure
- Health care
- Education
- Energy
- Homeland security
- Law enforcement

Where is the money going?



Source:
<http://www.recovery.gov/?q=content/investments>

Investments by Agency (Partial)

| Agency | Available ▼ | Paid Out |
|---|----------------|--------------|
| | \$ (Thousands) | |
| Department of Education (ED) | \$55,124,668 | \$12,397,257 |
| Department of Health and Human Services (HHS) | \$41,796,221 | \$25,856,312 |
| Department of Labor (DOL) ‡ | \$23,868,953 | \$13,864,891 |
| Department of Transportation (DOT) | \$23,359,369 | \$1,146,688 |
| Social Security Administration (SSA) | \$13,112,531 | \$13,101,076 |
| Department of Energy (DOE) | \$9,025,316 | \$281,883 |
| Department of Housing and Urban Development (HUD) | \$7,419,677 | \$988,041 |
| Environmental Protection Agency (EPA) | \$5,943,374 | \$41,656 |
| Department of Agriculture (USDA) | \$4,238,851 | \$3,212,598 |
| Department of Justice (DOJ) | \$3,112,318 | \$687,168 |
| Department of Defense (DOD) | \$1,725,219 | \$57,901 |
| Department of Treasury (TREAS) | \$1,473,445 | \$77,459 |
| General Services Administration (GSA) | \$1,375,580 | \$40,040 |
| National Science Foundation (NSF) | \$1,244,938 | \$16,872 |
| Department of Commerce (DOC) | \$1,068,756 | \$479,083 |
| US Army Corps of Engineers (USACE) | \$907,392 | \$109,391 |
| Department of Homeland Security (DHS) | \$694,600 | \$62,345 |
| Department of Veterans Affairs (VA) | \$577,245 | \$468,629 |



Breakdown for healthcare

- \$86.6 B - Medicaid
- \$24.7 B – COBRA subsidies
- \$19 B - HIT
- \$11.1 B - Research and NIH
- \$1.3 B - Military Service members' care
- \$1 B – Wellness and Prevention
- \$1 B - VHA
- \$2 B – Community Health
- \$500 M – Training
- \$500 M – Indian Health Service

Source:
http://en.wikipedia.org/wiki/American_Reinvestment_and_Recovery_Act



Major HITECH Provisions

\$19 B for health
information
technology

- Establishes an Office of the National Coordinator for Health Information Technology (ONCHIT);
- Establishes HIT Policy and Standards Committees;
- Requires HHS to develop initial HIT standards by 2010;
- Establishes incentives for the broad adoption of electronic health records;
- ***Improves and expands federal privacy and security protections for health information.***



Major Subtitle D Provisions

Subtitle D: Privacy and Security

- HIPAA privacy and security regulations expanded and applied directly to business associates;
- Defines breach of unsecured PHI and notification requirements;
- Modifies patient rights for requests for restrictions, access to medical records, and accounting of disclosures;
- Updates rules around marketing and the use of PHI;
- Increases civil monetary penalties for HIPAA violations.

Regulatory Timeline

1/1/09

4/1/09

7/1/09

10/1/09

12/31/09

9/17/2009

February 17, 2009

- ARRA signed
- State Attorney General enforcement

April 18, 2009

- HHS issues guidance regarding secured and unsecured data

August 19, 2009

- HHS and FTC issues interim regulations for breach notification

September 23, 2009

- Final breach notification requirements become effective

Regulatory Timeline

1/1/10

1/1/11

1/1/12

12/31/12

9/17/2009

February 18, 2010

- HIPAA Privacy and Security provisions extended to business associates
- Patient rights modified for restrictions and access to medical records
- Provisions modified for marketing and fundraising

January 1, 2011

- Patient right modified for accounting of disclosures

February 17, 2011

- Regulations established around sale of PHI
- Revised civil monetary penalties



Breach Notification

- Highlight
 - Guidance provided in April 2009 on methods to make PHI “unreadable” or “unusable”;
 - Use of encryption for electronic PHI;
 - Shredding or destruction for paper or electronic media;
 - Notification must occur in the event of a breach of “unsecured” PHI
 - Written notice must be provided to affected the individual(s) within 60 days;
 - HHS must be notified immediately for breaches involving 500 or more individuals; and, annually for all other breaches.
- Impact/Risk
 - Defining “breach” and “discovery”;
 - Record keeping of breach activity;
 - Publicity/Trust
 - Identification of risk areas; cost to mitigate risk



Business Associates

- Highlight
 - HIPAA Privacy and Security regulations, penalties and sanctions applied directly to Business Associates;
- Impact/Risk
 - Contract or BAA updates
 - BA compliance programs



Request for Restrictions

- Highlight
 - Individuals may request restrictions [with which the covered entity must comply] on disclosure of PHI to a health plan if the provider has been paid by the individual;
 - Exceptions include disclosures required for treatment or required by law.
- Impact/Risk
 - Flags for disclosure restrictions
 - Process impacts



Access to Medical Records

- Highlight
 - Individuals may request copies of records be provided in electronic format;
- Impact/Risk
 - EHR technology
 - Define “electronic” (e.g., CD, DVD, messaging, etc.)
 - Potential breach risks if not tightly controlled



Accounting of Disclosures

- Highlight
 - Must log disclosures for treatment, payment, and operations for prior 3 years and make available upon request by the patient;
- Impact/Risk
 - Effective dates impacted by date of EHR acquisition
 - Logging processes and data storage



Civil Monetary Penalties

- Highlight
 - Increased/tiered minimum penalties;
 - From \$100 to \$50,000 (per)
 - Total penalties max out between \$25,000 and \$1,500,000 depending on knowledge and/or intent;
 - Funds retained and/or provided to complainants to further enforce privacy and security requirements;
 - State Attorney General can now bring civil actions;
- Impact/Risk
 - Increased enforcement activity/auditing
 - Enhances current requirements, such as risk assessment
 - Patients could address concerns both at state or federal levels



Notable Events

- Increased federal funding for privacy and security audits;
- Security Rule administration and enforcement authority delegated to the OCR from OESS;
- Hiring of federal privacy staff;
- Involvement of FTC in publishing breach notification rules for PHR vendors.



Recommended next steps

- Conduct organizational awareness of ARRA and HITECH;
- Conduct a HIPAA v. HITECH regulatory gap analysis;
 - Current state v. required state;
 - Prioritize updates based on timetable;
 - Coordinate and implement policy and procedure updates;
 - Identify and coordinate technical updates;
- Conduct audit following major timetable milestones to assess compliance.



Wrap-Up

Andy Reeder, CISSP, CISA
Director, HIPAA Privacy and Security
Rush University Medical Center
Chicago, IL
312-942-2995 (o)
andrew_reeder@rush.edu