Enforce federal civil rights laws and the HIPAA Privacy and Security Rules
HQ and 10 Regional Offices
Region IX has jurisdiction over covered entities in Arizona, California, Hawaii, Nevada and the US Pacific Territories
Top 5 Privacy Rule complaint issues are impermissible uses/disclosures, safeguards, access, minimum necessary and notice.

Top Large Breach Notification reasons include theft, loss, and unauthorized access.

In 2011, OCR received 9032 complaints.

Increased Enforcement with CMP and Resolution Agreements with Monetary Settlements of $1M or more since 2009.
The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, is designed to promote the widespread adoption and standardization of health information technology, and requires HHS to modify the HIPAA Privacy, Security, and Enforcement Rules to strengthen the privacy and security protections for health information and to improve the workability and effectiveness of the HIPAA Rules.
Breach Notification IFR

- Guidance issued 4/17/2009
  - Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
- IFR issued 8/24/2009
  - Effective for breaches after 9/23/09
  - 120 comments received
### Enforcement IFR

- **IFR issued 10/30/2009**
- **25 Comments Received**

<table>
<thead>
<tr>
<th></th>
<th>For violations occurring prior to 2/18/2009</th>
<th>For violations occurring on or after 2/18/2009</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PENALTY AMOUNT</strong></td>
<td>Up to $100 per violation</td>
<td>From $100 to $50,000 per violation</td>
</tr>
<tr>
<td><strong>CALENDAR YEAR CAP FOR</strong></td>
<td>$25,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td><strong>VIOLATIONS OF AN IDENTICAL PROVISION</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HITECH NPRM

- NPRM issued 7/14/2010
- 304 Comments Received
HITECH Sections 13401 and 13404 make BAs accountable to consumers and to HHS for protecting the privacy and security of protected health information and directly liable for criminal and civil penalties for violations of certain provisions of the HIPAA Privacy and Security Rules.
NPRM proposes:

- Requiring that BAs comply with the technical, administrative, and physical safeguard requirements under the Security Rule.
- Prohibiting a BA from making a use or disclosure in violation of the Privacy Rule.
- Including Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities as BAs.
- Clarifying that BAs are liable whether or not they have an agreement in place with the CE.
- Defining subcontractors as BAs; clarifying that BA liability flows to all subcontractors.
HITECH Section 13405(d) explicitly bans the sale of protected health information without authorization.
NPRM proposes:

- Prohibiting a CE or BA from selling PHI without authorization.
- Including Specific Exceptions to this General Prohibition
HITECH Section 13406(a) tightens the HIPAA Privacy Rule’s marketing provisions by now requiring authorizations for certain health-related communications to the individual that are paid for by a third party.
NPRM proposes:

- Requiring authorizations for health-related communications (except for treatment) about the CE’s products or services, case management or care coordination, and treatment alternatives where the CE receives payment in exchange for making the communication from or on behalf of the third party whose product or service is being described.
- Limited exception for refill reminders.
- For subsidized treatment communications, requiring that health care providers notify patients of the fact of remuneration and provide an opportunity for patients to opt out of receiving such communications.

CEs can still engage in face to face communications about products or services with an individual or provide promotional gifts of nominal value to an individual without an authorization.
HITECH Section 13406(b) ensures that individuals will have a clear and conspicuous opportunity to opt out of all fundraising communications sent by or on behalf of a covered entity.
NPRM proposes:

- Requiring that each fundraising communication to an individual include a clear and conspicuous opt-out method that would not cause the individual to incur an undue burden or more than a nominal cost.
- Prohibiting a covered entity from sending further fundraising communications to an individual who has opted-out.
- Prohibiting a covered entity from conditioning treatment or payment on the individual’s choice to opt-out.
HITECH Section 13405(e) strengthens individuals’ right to access their protected health information by creating an absolute right to an electronic copy of their health information if the entity maintains the information electronically.
NPRM proposes:

- Strengthening the right to an electronic copy of PHI in any electronic designated record set, not just in an electronic health record.
- Permitting a covered entity to charge a reasonable, cost-based fee to cover the labor for copying and electronic media.
- Giving an individual the right to direct the covered entity to transmit the copy of protected health information directly to another person designated by the individual.
HITECH Section 13405(a) strengthens the HIPAA Privacy Rule’s individual rights by requiring a health care provider to comply with an individual's requested restriction not to disclose health information about a particular health care service to a health plan for payment or health care operations, as long as the individual has paid the provider out of pocket in full and has requested such a restriction.
NPRM proposes that a covered entity must abide by the requested restriction regardless of whether it is the individual paying out of pocket for the health care service or item or whether a family member or other person is paying for the care on behalf of the individual.
HITECH Section 13405(b) provides:
• CEs must first consider whether a limited data set is sufficient as “minimum necessary” to accomplish a particular purpose; and
• Requires the Department to issue guidance on what constitutes “minimum necessary”.
• The guidance sunsets the provision.
NPRM does not include proposed regulatory text to implement this HITECH Act provision but explains that HHS intends to issue the required guidance based on the public input received, which would negate the need for a change in the Privacy Rule.
NPRM proposes to modify the HIPAA Enforcement Rule regarding:

- Willful neglect;
- The definition of reasonable cause;
- The factors used in determining a civil money penalty amount; and
- Affirmative defenses.
Proposed Compliance Dates

- Covered entities and business associates will have 180 days from the effective date of the final rule to comply.
- Covered entities and business associates will have up to one year from the compliance date (one year and 240 days from the publication date) to make any necessary changes to existing business associate agreements.
  - Sooner if agreement is renegotiated during this time period.
  - Business associates must still comply with all other applicable requirements of the HIPAA Rules, even if not reflected in agreement.
Final HITECH Rule: Timeline

- Final HITECH Modifications, Final Breach Rule, Final Enforcement Rule, and Final Genetic Information Nondiscrimination Act (GINA) Rule will be issued together
  - Minimizes staggered compliance dates
  - Minimizes changes to notices of privacy practices
- Final Omnibus Rule expected soon
Accounting of Disclosures

- Disclosures for treatment, payment, health care operations
- “Through an electronic health record”
- Balance interests of individuals and administrative burden on covered entities
- NPRM expected soon
National Outreach Campaign

- Digital toolkit of consumer materials
  - Backgrounders with general information
  - Fact sheets on specific topics
  - Videos on specific topics
- Community discussions on EHRs
- Improved website navigation
Audit Program

- HITECH grants OCR the authority to conduct periodic audits of covered entities and business associates.

State Attorneys General Training

- Education on HIPAA
- Plan for coordination of investigations
Questions?
For More Information

- OCR Website: [http://www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy)
- OCR List serve