



Compliance and Enforcement of the Privacy Rule





Compliance Date

- ◆ April 14, 2003 – Compliance for all but small health plans
- ◆ One year extension for small health plans
- ◆ No statutory extension available in Privacy Rule, unlike extension available for Transaction Rule through 10/16/03



Office for Civil Rights

- ◆ Enforces Civil Rights laws and the Privacy Rule
- ◆ With respect to the Privacy Rule:
 - Promote voluntary compliance
 - Investigation and Resolution of Complaints
 - Exception Determinations



Why Voluntary Compliance?

- ◆ Promoted by HIPAA statute and Privacy Rule
 - Education, Cooperation, Technical Assistance
 - Permitted even after investigation commences
 - Can help mitigate CMPs
- ◆ Most efficient way to promote privacy

42 USC §1320d-5, §160.304



Technical Assistance

- ◆ Integrated Rule and Preambles to Dec. 2000, Aug. 2002 Final Rules
- ◆ Covered Entity decision tool
- ◆ December 4, 2002 Guidance
- ◆ Targeted Technical Assistance materials under development
- ◆ Fact sheet on August 2002 modifications
- ◆ Sample Business Associate Contract
- ◆ FAQs on our website
- ◆ <http://www.hhs.gov/ocr/hipaa/>



December 4, 2002 Guidance

- ◆ General Overview
- ◆ Incidental Uses and Disclosures
- ◆ Minimum Necessary
- ◆ Personal Representatives
- ◆ Business Associates
- ◆ Uses and Disclosures for Treatment, Payment and Health Care Operations
- ◆ Marketing
- ◆ Public Health
- ◆ Research
- ◆ Workers' Compensation Laws
- ◆ Notice
- ◆ Government Access
- ◆ Miscellaneous FAQs



Investigations & Compliance Reviews

- ◆ OCR may investigate complaints
- ◆ OCR may conduct compliance reviews to determine whether Covered Entities are in compliance



Filing Complaints

- ◆ Any person or organization may file complaint with OCR by mail or electronically
 - Only for possible violations occurring after compliance date
 - Complaints should be filed within 180 days of when the complainant knew or should have known that the act or omission occurred
- ◆ Individuals may also file complaints with Covered Entity



Complaint Process

- ◆ Informal review may resolve issue fully without formal investigation
 - Many complaints will be resolved at this stage
- ◆ If not, begin investigation
 - Voluntary resolution yet possible
- ◆ Technical Assistance



Civil Monetary Penalties (CMPs)

- ◆ CMPs can be imposed by OCR:
 - \$100 per violation
 - Capped at \$25,000 for each calendar year for each identical requirement or prohibition that is violated
 - Covered Entity has a right to notice and a hearing before a CMP becomes final

42 USC §1320d-5



No CMPs if:

- ◆ Person did not know – and by exercising reasonable diligence would not have known - of the violation
- ◆ If failure to comply is due to reasonable cause and not willful neglect and entity corrects within 30 day cure period
- ◆ Offense is punishable by criminal sanction



CMP Flexibility Summary

- ◆ Exceptions
- ◆ Potential extension of the 30 day cure period
- ◆ CMP reduction possible if:
 - Amount excessive relative to violation
 - Due to reasonable cause/not willful neglect



Criminal Penalties for Wrongful Disclosures

- ◆ For knowingly obtaining or disclosing identifiable health information relating to an individual in violation of the Rule:
 - Up to \$50,000 & 1 year imprisonment
 - Up to \$100,000 & 5 years if done under false pretenses
 - Up to \$250,000 & 10 years if intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm
- ◆ Enforced by DOJ



Additional Information

www.hhs.gov/ocr/hipaa/

OCR Privacy Toll Free Number:
(866) 627-7748