



HIPAA Privacy Rule Enforcement

Marilou King, JD

Office for Civil Rights, HHS

Fourteenth National HIPAA Summit

March 29, 2007

Enforcement Results

(4/14/2003 to 12/31/2006)

- Complaints received 24,000 (approx.)
- Complaints open 5,469
- **Complaints concluded 18,529 (77% of receipts)**
- Referrals to DOJ 362 (39 accepted)
- Enforcement results are measured by looking at the “**Complaints Concluded**” category and the outcomes of the enforcement process.

Enforcement Results

(4/14/2003 – 12/31/2006)

- Investigated Cases 5,987 (32% of closures)
 - Found no violation 1,972 (33% of investigations)
 - Obtained corrective action 4,015 (67% of investigations)
(OCR obtains satisfactory voluntary compliance, corrective action, and/or provides technical assistance resulting in change in the covered entity's privacy policies and practices)

- Concluded after preliminary review 12,542 (67% of closures)
(lack of jurisdiction, timeliness, consents or allegations that would be a failure to comply with Privacy Rule)

- Total 18,529

Enforcement Results

(4/14/2003 – 12/31/2003)

- Investigated Cases 339 (23% of closures)
 - Found no violation 79 (23% of investigations)
 - Obtained corrective action 260 (77% of investigations)
(OCR obtains satisfactory voluntary compliance, corrective action, and/or provides technical assistance resulting in change in the covered entity's privacy policies and practices)

- Concluded after preliminary review 1,169 (77% of closures)
(lack of jurisdiction, timeliness, consents or allegations that would be a failure to comply with Privacy Rule)

- **Total 1,508**

Enforcement Results

(01/01/2004 – 12/31/2004)

- Investigated cases 1,392 (30% of closures)
 - Found no violation 359 (26% of investigations)
 - Obtained corrective action 1,033 (74% of investigations)
(OCR obtains satisfactory voluntary compliance, corrective action, and/or provides technical assistance resulting in change in the covered entity's privacy policies and practices)

- Concluded after preliminary review 3,372 (70% of closures)
(lack of jurisdiction, timeliness, consents or allegations that would be a failure to comply with Privacy Rule)

- Total 4,764

Enforcement Results

(01/01/2005 – 12/31/2005)

- Investigated Cases 1,803 (33% of closures)
 - Found no violation 642 (36% of investigations)
 - Obtained corrective action 1,161 (64% of investigations)
(OCR obtains satisfactory voluntary compliance, corrective action, and/or provides technical assistance resulting in change in the covered entity's privacy policies and practices)

- Concluded after preliminary review 3,818 (67% of closures)
(lack of jurisdiction, timeliness, consents or allegations that would be a failure to comply with Privacy Rule)

- Total 5,621

Enforcement Results

(01/01/2006 – 12/31/2006)

- Investigated Cases 2,466 (39% of closures)
 - Found no violation 895 (36% of investigations)
 - Obtained corrective action 1,571 (64% of investigations)
(OCR obtains satisfactory voluntary compliance, corrective action, and/or provides technical assistance resulting in change in the covered entity's privacy policies and practices)

- Concluded after preliminary review 4,001 (61% of closures)
(lack of jurisdiction, timeliness, consents or allegations that would be a failure to comply with Privacy Rule)

- Total 6,467

Enforcement Results

(continued)

- Change has been obtained by HHS/OCR in the privacy practices and procedures of over 4,000 investigated entities – 67% of investigations.
- These changes are the result of an active enforcement program designed to seek voluntary compliance and corrective action to obtain systemic change in the health industry.
- Systemic change through voluntary compliance and corrective action has increased.
- No violation determinations have increased.
- Cases ineligible for investigation have decreased but remain a considerable number.
- Successful enforcement results are achieved case by case. Some case examples follow.

Enforcement Cases

- **Pharmacy Chain Institutes New Safeguards for Protected Health Information**

Pharmacy stores maintained pseudoephedrine log books containing protected health information so that individual protected health information was visible on counter. OCR required that CE implement new training and national policies and procedures to safeguard the log books.

Enforcement Cases

- **Health System Changes System-wide Process for Amendment of Records**

Health system failed to consider a request for amendment without an appeal to legal counsel's office. As a condition for resolution, OCR required the CE to revise its policies and procedures to eliminate this step, and to implement the change nationally.

Enforcement Cases

- **Provider Revises Process to Prevent Unauthorized Disclosures to Employers**

Physician's office disclosed protected health information to complainant's employer without compliant authorization. OCR required the CE to revise its policies and procedures to require compliant patient authorization prior to release protected health information to an employer. All staff was trained on the revised policies and procedures.

HHS Approach to Enforcement

- HHS enforces the requirements of the Privacy Rule every day through investigations of covered entities.
- Responses by covered entities to OCR enforcement result in change that is systemic and affects all individuals served by the entity.
- The imposition of civil money penalties (CMPs) is one enforcement tool. This enforcement tool is exercised when satisfactory resolution is not obtained. HHS will impose CMPs in appropriate cases.
- HHS has been successful to date in obtaining satisfactory change in all investigated cases where noncompliance is indicated.
- Change has come through the voluntary responses of covered entities and has been obtained more quickly and with less adversarial process than the imposition of money penalties.

Why Has HHS Adopted this Approach?

- Most effective way to obtain industry compliance with the Privacy Rule.
- Most prompt for all: complainants, covered entities, and OCR.
- Most efficient use of enforcement resources.
- Resolution must be satisfactory to the Secretary.

45 CFR 160.312- Secretarial Action regarding Complaints and Compliance Reviews

- If an investigation indicates noncompliance, the Secretary will attempt to reach a resolution satisfactory to the Secretary by informal means.
- Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.
- If the matter is not resolved by informal means, then a penalty may be imposed through a Notice of Proposed Determination.

Issues in Enforcement Actions

The compliance issues investigated most frequently, in order, are:

- Impermissible uses and disclosures of protected health information;
- Safeguards;
- Access of patients to their protected health information;
- Minimum necessary uses of protected health information; and
- Authorizations.

Covered Entities in Enforcement Actions

The most common types of covered entities that have been required to take corrective actions and voluntarily comply, in order of frequency, are:

- Private physician practices;
- General hospitals;
- Outpatient facilities;
- Pharmacies; and
- Group health plans.