



HCCA's 12th ANNUAL COMPLIANCE INSTITUTE

APRIL 13-16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

Update on Enforcement of the
HIPAA Privacy and Security Rules

Marilou King, JD
Office for Civil Rights
U.S. Department of Health and Human Services



www.hcca-info.org | 888-580-8373



Privacy Rule - Complaint Investigations

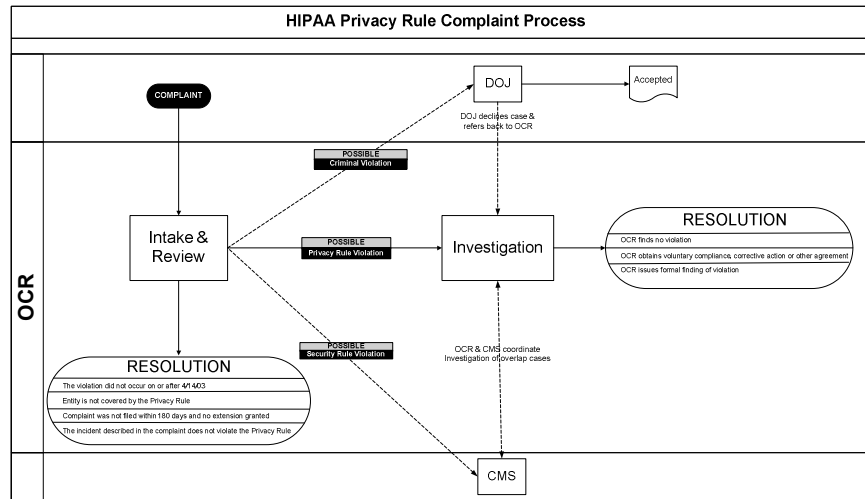
- Every complaint received by OCR is reviewed and allegations analyzed
- An investigation is launched when warranted by the allegations in the complaint
- OCR investigations have resulted in changes and improvements in the privacy practices and procedures of covered entities in over 5,500 cases since April 2003
- Corrective action obtained by HHS from covered entities has resulted in systemic change that benefits all individuals they serve



www.hcca-info.org | 888-580-8373

2

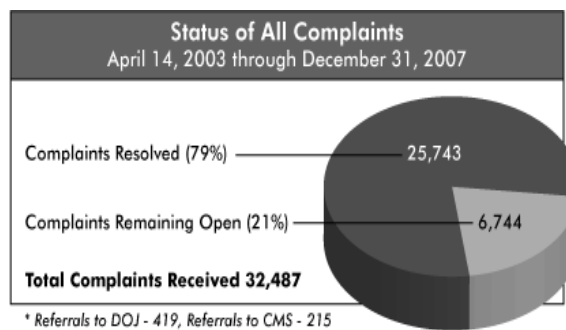
Privacy Rule - Complaint Process



www.hcca-info.org | 888-580-8373

3

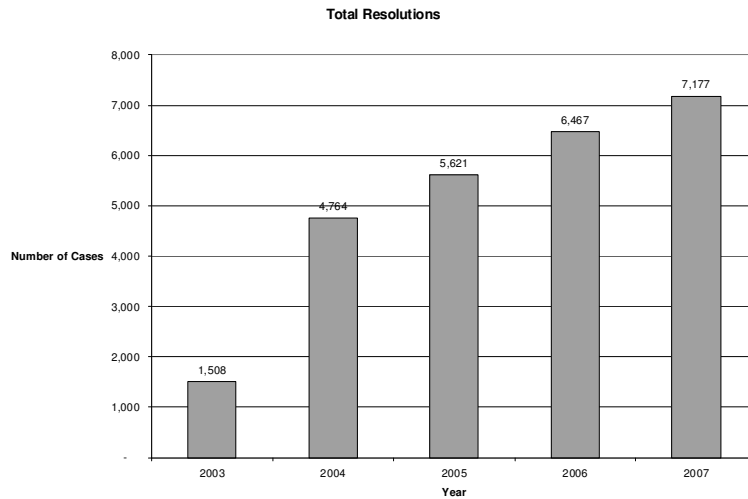
Privacy Rule - All Complaints



www.hcca-info.org | 888-580-8373

4

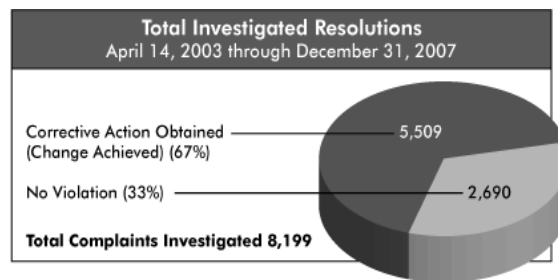
Privacy Rule - Complaints Resolved by CY



www.hcca-info.org | 888-580-8373

5

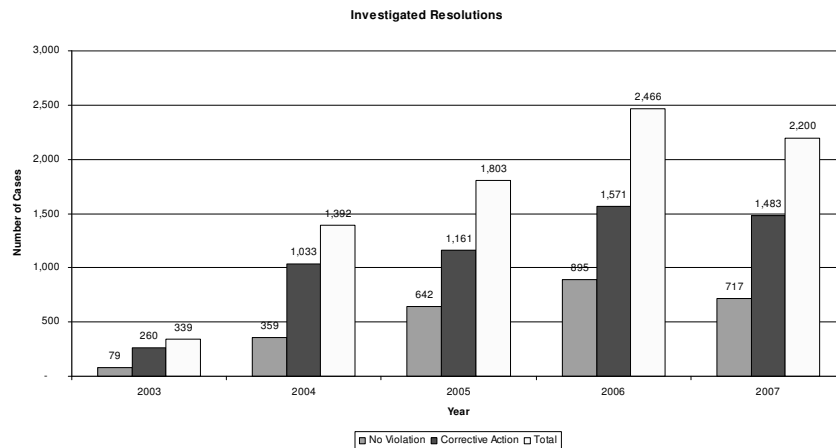
Privacy Rule - Total Investigated Cases



www.hcca-info.org | 888-580-8373

6

Privacy Rule - Investigated Cases by CY



www.hcca-info.org | 888-580-8373

7

Privacy Rule - Issues in Enforcement Actions

(April 14, 2003 to December 31, 2007)

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

- Impermissible use or disclosure of an individual's identifiable health information
- The lack of adequate safeguards to protect identifiable health information
- Refusal or failure to provide the individual with access to or a copy of his/her records
- The disclosure of more information than is minimally necessary to satisfy a particular request for information
- Failure to have the individual's valid authorization for a disclosure that requires one



www.hcca-info.org | 888-580-8373

8

Privacy Rule - Covered Entities in Enforcement Actions

(April 14, 2003 to December 31, 2007)

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
- Health plans (Group Health Plans and Health Insurance Issuers)
- Pharmacies

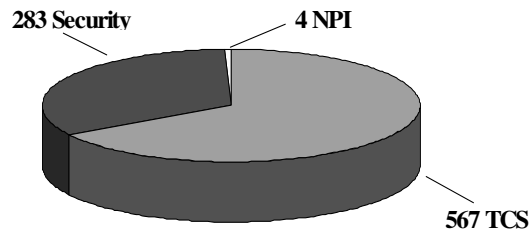


www.hcca-info.org | 888-580-8373

9

CMS HIPAA Complaint Statistics

(as of December 31, 2007)



Complaint Type	Open	Closed	Totals
Transactions and Code Sets (TCS)	52	515	567
Security	92	191	283
National Provider Identifier (NPI)	0	4	4
Total	144	710	854

Note: 49 of 191 of the closed Security Rule cases have been resolved through corrective actions by the covered entities.



www.hcca-info.org | 888-580-8373

10

Top Security Rule Complaint Issues

- Unauthorized access to ePHI
 - For example, employees or relatives access ePHI inappropriately
- Loss or theft of devices containing ePHI
 - Small number of complaints, large volume of ePHI
- Insufficient access controls for systems
 - Shared passwords, generic user IDs, lack of encryption
- Majority of Security Rule complaints are referred to CMS by OCR; originated as Privacy Rule complaints



www.hcca-info.org | 888-580-8373

11

Privacy Rule - Enforcement Case Examples

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

Pharmacy stores maintained pseudo ephedrine 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.



www.hcca-info.org | 888-580-8373

12

Privacy Rule - Enforcement Case Examples

- **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.



www.hcca-info.org | 888-580-8373

13

Privacy Rule - Enforcement Case Examples

- **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.



www.hcca-info.org | 888-580-8373

14

Privacy Rule - Enforcement Case Examples

- **National Health Insurer Required to Sanction Employee, Retrain Staff and Mitigate Harm**

An employee of a major health insurer impermissibly disclosed the protected health information of one of its members without following the insurer's authorization and verification procedures. OCR required the health insurer to:

- train its staff on the applicable policies and procedures;
- mitigate the harm to the individual; and
- apply sanctions to employee who made the unauthorized disclosure



www.hcca-info.org | 888-580-8373

15

Privacy Rule - Enforcement Case Examples

- **HMO Required to Correct Computer Program**

A national health maintenance organization sent explanation of benefits (EOB) by mail to a complainant's unauthorized family member. OCR's investigation determined that a flaw in computer program put the protected health information of approximately 2,000 families at risk of disclosure in violation of the Rule. OCR required the insurer to:

- correct the flaw in its computer program;
- review all transactions for a six month period; and
- correct all corrupted patient information.



www.hcca-info.org | 888-580-8373

16

Security Rule – Enforcement Case Example

- **Provider and its Business Associate Required to Correct Website Program**

A small provider allowed patients to register on-line, using an internet service. The program allowed any user of the website to see ePHI of all of the registered users. CMS investigation determined that flaw in website program put ePHI of approximately 500 individuals at risk of disclosure.

- CMS/OESS required the covered entity to:
 - Immediately correct the flaw in the website application;
 - Monitor the website daily to ensure the program was corrected



www.hcca-info.org | 888-580-8373

17

Other Avenues to Obtain Compliance

- Resolution Agreements are next step in enforcement actions.
- Where informal resolution through voluntary compliance, corrective action, or Resolution Agreement satisfactory to HHS is not reached with the covered entity, next stage is Notice of Proposed Determination containing a civil money penalty.
- HHS also obtains privacy compliance through outreach and education efforts. HHS has reached hundreds of thousands of covered entities and consumers through educational conferences, a toll-free call line, and an interactive website.



www.hcca-info.org | 888-580-8373

18

Security Rule – Compliance Reviews

- In 2008, CMS will conduct on-site compliance reviews.
- CMS has contracted with PriceWaterhouseCoopers to conduct reviews.
- Reviews will be conducted on covered entities against whom complaints has been filed; selection will be based on a severity impact analysis – where violation had the potential to affect a large number of individuals.
- CEs will be required to produce a list of mandatory documentation, such as the risk assessment and risk management plans; specific policies and procedures; and samples of training and awareness materials.
- All compliance reviews will include assessment of policies and procedures related to remote access and use of portable devices.
- CMS will publish “lessons learned” from the reviews on the CMS website: www.cms.hhs.gov/enforcement.



www.hcca-info.org | 888-580-8373

19

Tips for Privacy and Security Compliance Officers Handling an OCR or OESS Investigation

- When notification letter is received, contact investigator named in letter. Establish effective communication with investigator. Contact investigator for assistance with questions, such as, “How does this work...?”
- Respond within stated time frames. If CE cannot make the due date, let investigator know. Request a reasonable extension of time – enough so CE can accomplish the requested task. Avoid multiple requests for time extensions. Return telephone calls from the investigator promptly.



www.hcca-info.org | 888-580-8373

20

Investigation Tips (cont'd)

- Understand that investigations take place over an extended period of time. The investigator will work hard to be timely but some investigations take longer than others.
- Be cooperative with the investigator. Facts need to be confirmed by OCR or OESS. If investigator requests to interview an employee or requests contact information for former employees, provide this information in a timely manner. If you cannot, explain why.
- Ask for technical assistance if you do not understand what is expected by a particular requirement of the Privacy Rule or Security Rule.



www.hcca-info.org | 888-580-8373

21

Investigation Tips (cont'd)

- If CE is aware of a Privacy Rule or Security Rule incident even before receiving notification letter, start gathering relevant materials and facts. Formulate a corrective action plan (CAP) and execute it. An executed CAP will then be in place to deliver to the investigator when the notification letter is received.
- Be specific in your responses to requests for data and information. For example, if training was provided, supply all the facts – when, who was trained (sign-in sheet), topics covered. If a policy was revised, send copy of old and new policies. Do not send entire privacy policies and procedures manual unless specifically requested.



www.hcca-info.org | 888-580-8373

22

Investigation Tips (cont'd)

- Be forthcoming and acknowledge errors if they occurred. Remember, the goal is resolution through voluntary compliance and completed corrective action.
- **Respond.** Ignoring the investigation will exacerbate the matter.



www.hcca-info.org | 888-580-8373

23

Our Mutual Goal

Ensuring the privacy and security of each individual's health information in accordance with the standards and requirements of the HIPAA Privacy and Security Rules.



www.hcca-info.org | 888-580-8373

24

Privacy Rule - Want More Information?

The OCR website, <http://www.hhs.gov/ocr/hipaa/> offers a wide range of helpful information about the Privacy Rule:

- The full text of the Privacy Rule
- A HIPAA Privacy Rule summary
- A covered entity "decision tool" to assist individuals and entities in making these determinations
- Over 200 frequently asked questions
- Fact sheets
- Information and monthly statistics about the OCR enforcement program



www.hcca-info.org | 888-580-8373

25

Security Rule – Want More Information?

The CMS website, <http://www.cms.hhs.gov> offers a wide range of helpful information about the Security Rule:

- The full text of the Security Rule
- Guidance on Remote Access
- Educational materials, including seven Security Papers focusing on each aspect of the Rule
- Frequently Asked Questions (FAQs)
- Information and monthly statistics about the OESS enforcement program



www.hcca-info.org | 888-580-8373

26