PrivacyStudio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 7
Specific US Privacy Laws and Regulated Data Types

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Seven
SPECIFIC US PRIVACY LAWS & REGULATED DATA TYPES

Personal Information of Children

The **Children's Online Privacy Protection Act of 2000** (COPPA) regulates the collection of personal information of children under 13 by commercial website operators.[130] The Federal Trade Commission has promulgated rules to implement COPPA, and it frequently brings actions against companies that have not complied with the COPPA requirements.

THE HERSHEY CASE (FEBRUARY 2003)[131]

Respondent: The Hershey Company

Regulator: Federal Trade Commission

Basis for Complaint: Violations of the Children's Online Privacy Protection Act of 1998 and Section 5 of the FTC Act

Facts and Allegations: Respondent is the maker and marketer of chocolate and confectionary products including the popular Mounds, Reese's, and KitKat brands. The company offered a special section on its corporate website directed at children under the age of 13. Known as "Kidztown", this section featured children's games, cartoon characters, and a "Candy of the Month" promotion. Hershey collected children's personal information from this portion of the website including: name, address, email address, gender, approximate age, and often telephone number.

Hershey also marketed a number of its products through individual websites dedicated to each candy brand. These websites similarly targeted and collected information from visitors including children.

Hershey and its affiliate branded websites managed a sweepstakes to give away free candy. Registration required parental consent. The parental consent form only required the name, home address, and the selection of the "I consent" box. Additionally, even if no information was entered in the parental forms and the child had indicated that he/she was under age 13, Hershey still accepted the registration. Sweepstakes winners' names and home states were published on the website without parental consent.

The FTC alleged that, in violation of COPPA and Section 5 of the FTC Act, Hershey operated a Web site directed at children and had actual knowledge that it collected personal information from children without sufficient parental consent, notice on its website, direct notice to parents of the information collected, and without providing reasonable means for parents to review/delete the information.

Outcome: The FTC entered into a consent decree with Hershey, ordering:

Bar on Misrepresentation: Must fully disclose information collection, use, and disclosure policies on the website and in direct parental notice.

Treatment of the Children's Personal Information: Hershey shall, within five days of the Consent Decree date, delete all personal information collected from children through its websites (other than information collected in compliance with COPPA).

Consumer Education Remedy: For five years, Hershey shall place a clear and conspicuous COPPA notice on its websites (within its privacy policy) and within the direct notice required to be sent to parents in boldface type directing them to the privacy policy statement online.

Maintenance of Relevant Documents: For a period of five years, Hershey shall provide (upon request):

(1) A copy of different information collection forms;
(2) Collection, use, and disclosure policies with regard to children; and
(3) Any document that contradicts, qualifies or questions Hershey's compliance with the order.

Delivery of Order: Within 30 days, Hershey shall deliver and obtain signed receipt of the FTC order along with the FTC compliance guide entitled "How to Comply with the Children's Online Privacy Protection Rule" with respect to each current (and for three years, future) director, employee, agent, representative, or employee with managerial responsibility.

Reporting: For 20 years, Hershey shall notify the FTC within 30 days of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Hershey shall file a report with the FTC setting forth its compliance with the order including:

(1) Information collection practices;
(2) Copy of different privacy notice on websites;
(3) Copy of parental privacy notices;
(4) How to obtain parental consent;
(5) How to provide opportunity for parents to review information collected; and
(6) Security, confidentiality, and integrity of personal data procedures.

Fine Imposed: $85,000

The Xanga case demonstrates the Federal Trade Commission's application of the COPPA rules to the operation of social networking sites that attract children.

THE XANGA CASE (SEPTEMBER 2006)[132]

Respondent: Xanga.com, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violations of the Children's Online Privacy Protection Act of 1998 and Section 5 of the FTC Act

Facts and Allegations: Respondent is a social networking website that was started in 1999 and is based in New York City. In 2005 it had approximately 25 million registered accounts. Xanga users are required to set up a personal profile which then allows them to post information about themselves and create personal pages or blogs containing profile information such as online journals, images, text, videos, *etc.* These profiles and personal pages are available for other users to read and respond to, and are also available to the general public through global search engines such as Google and Yahoo.

Xanga's website terms of use policy stated that children under age 13 could not join. However, over a period of five years, Xanga created 1.7 million accounts for (and collected and disclosed personal information from) users who indicated they were under age 13.

The FTC alleged that Xanga violated the Children's Online Privacy and Protection Act, the COPPA Rule and the FTC Act by knowingly collecting personal information from children under the age of 13 and by failing to:

(1) Provide notice to parents of information collection practices;

(2) Obtain parental consent prior to collecting, using & disclosing children's personal information online; and

(3) Provide parents with reasonable means to access and control their children's information.

Outcome: The FTC entered into a consent decree with Xanga, ordering that all websites and online services operated by Xanga and its principals shall comply with COPPA and applicable FTC Rules. Additionally, within five days from the entry of the Consent Decree, Xanga shall delete all personal information collected and maintained in violation of COPPA through the date of the order.

For five years, Xanga shall place on its homepage(s) and privacy notice(s) a clear and conspicuous notice in boldface type regarding the FTC's program for protecting children, along with a hyperlink to the FTC's website. An additional notice to parents regarding children and social networking sites must be included:

(1) Within the privacy policy required to be posted on its website;

(2) Within the direct notice required to be sent to parents in boldface type directing them to the privacy policy statement online; and

(3) In boldface type and in the form of a hyperlink at each location on its website(s) that collects personal information.

Maintenance of Relevant Documents: For a period of five years, Xanga shall provide (upon request and within 14 days) all documents demonstrating compliance with the terms and provisions of the Consent Decree.

Delivery of Order: Within 30 days, Xanga shall deliver and obtain a signed receipt of both the FTC order and the FTC COPPA compliance guide with respect to each of the principals, officers, directors, and managers, and to all employees, agents, and representatives having responsibilities related to this order; a list of these names should be submitted to the FTC within 10 days of complying with the order along with a statement setting forth its compliance. Delivery of the same is required for five years to all future directors, officers, agents, and managerial employees.

Reporting: For 3 years, the FTC shall be notified (1) by the individual defendants within 10 days of any changes in addresses or telephone numbers, employment or business ownership, or names and aliases; and (2) by Xanga 30 days prior to any changes in corporate structure which may affect its compliance with the order.

Within 60 days after service of the order and thereafter as requested, Xanga and the other individual defendants shall file reports with the FTC setting forth their compliance with the order including:

(1) Current residential and businesses addresses and telephone numbers, and descriptions of business activities and responsibilities of the individual defendants;

(2) Statement of website registration criteria and process, and copies of pages that provide/collect registration information;

(3) Copy of all privacy notices posted on Xanga's websites, and a statement detailing the location of the notices along with copies of the pages that collect personal information;

(4) Copy of all privacy notices sent to parents, and a statement detailing when and how the notices were provided;

(5) Statement detailing the methods used to obtain parental consent prior to the collection and use of children's personal information;

(6) Statement detailing the means provided for parents to access and control their children's personal information;

(7) Statement detailing the reasonable necessity for collecting each type of information from a child; and

(8) Statement detailing the procedures used to protect the personal information collected from children.

Fine Imposed: $1,000,000

State attorneys general can also bring COPPA actions.

THE SANTA.COM CASE (DECEMBER 2007)[133]

Respondent: Small's Seed Company, LLC

Regulators: Texas State Attorney General

Basis for Complaint: Violations of the Texas Deceptive Trade Practices-Consumer Protection Act and the Children's Online Privacy Protection Act (COPPA)

Facts and Allegations: Respondent maintains a website "Santa.com" that allowed children to make Christmas wish lists, write e-mails to Santa, play games, and read blogs from Santa and his reindeer, among other things. The Texas Attorney General alleged that the website collected personal information from children under 13 years of age in violation of COPPA. The Texas Attorney General also alleged that the respondent made false, deceptive or misleading statements about its collection of information from children on the website and failed to clearly and conspicuously disclose all material information regarding its information collection practice, as required by the Texas Deceptive Trade Practice law.

Outcome: Although respondent denied the allegations above, it agreed to enter into an Assurance of Voluntary Compliance, providing that will:

(1) Make no misrepresentation regarding its information handling practices;

(2) Comply with COPPA, by (for example) providing COPPA-required notices on its home page and those pages that collect personal information from children under 13, obtaining verifiable parental consent prior to collecting information from such children, and not requiring such children to provide personal information except as necessary to participate in the activities offered; and

(3) Delete any information collected previously from children under 13 in a way that did not comply with COPPA.

Fine Imposed: None

Consumer Reporting Data and Credit Information

The **Fair Credit Reporting Act (FCRA)** regulates the collection, disclosure and use of any third-party information used to make decisions about consumers' eligibility for credit, insurance, employment, government benefits and other purposes, such as residential housing.

The Federal Trade Commission has promulgated rules to implement the Fair Credit Reporting Act as applied to consumer reporting agencies, users of consumer reports and entities that furnish data to consumer reporting agencies.

Financial institutions outside of the Federal Trade Commission's jurisdictions, receive FCRA compliance oversight from their Federal financial institution regulators. The FCRA is also enforced by state attorneys general, state insurance company regulators, and through private lawsuits.

THE CHOICEPOINT CASE (JANUARY 2006)[134]

Respondent: ChoicePoint, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Fair Credit Reporting Act (FCRA)

Facts and Allegations: Respondent is a Georgia-based data broker that collects and sells consumer reports and other consumer data to businesses, professionals and government agencies that use the data for risk management, FCRA permissible purposes such as insurance underwriting and employment, and other purposes. These entities must apply to become ChoicePoint subscribers. The applications are processed in order to establish that the applicant is a legitimate organization and has an appropriate, permissible purpose for purchasing the consumer data. Once the applicant is approved as a subscriber, it may access consumer data from ChoicePoint, including consumer reports.

In early 2004, ChoicePoint discovered that sensitive personal information of approximately 145,000 consumers had been disclosed to persons who lacked a proper purpose to obtain such information. According to the FTC, the information was obtained by criminals who had posed as legitimate business and been approved as subscribers based on applications containing false information and other misrepresentations.

The FTC alleged that ChoicePoint failed to have reasonable procedures in place to screen potential subscribers, causing it to fail to detect the false information and other misrepresentations in the applications. As a result, ChoicePoint violated the Fair Credit Reporting Act by:

- Furnishing consumer reports to subscribers who did not have a permissible purpose;
- Failing to first make a reasonable effort to verify the identity of the prospective user and its intended uses of the consumer reports;

- Continuing to furnish consumer report when it had reasonable grounds for believing the consumer report would not be used for a permissible purpose; and

- Failing to monitor and identify unauthorized activity after being alerted of fraudulent activity from authorities between 2001 and 2005.

The FTC alleged that ChoicePoint also violated the FTC Act by failing to use reasonable and appropriate measures to protect the security of sensitive personal information and that this failure caused or is likely to cause substantial injury to consumers. The FTC classified these acts and practices as unfair or deceptive under Section 5 of the FTC Act.

Outcome: The FTC entered into a consent decree with ChoicePoint, ordering:

Bar on Misrepresentation: ChoicePoint shall not misrepresent the manner or extent to which it maintains and protects the privacy, confidentiality or security of the personal information it collects.

FCRA-related Provisions: ChoicePoint is permanently restrained from furnishing consumer reports to persons who do not have a permissible purpose; therefore it must maintain reasonable procedures to ensure that consumer reports are provided only to those with a permissible purpose. These procedures include (1) obtaining written certification from each subscriber describing the nature of its business and specific intended permissible purpose for using consumer data, (2) verifying the subscribers' identity and the legitimacy of its business and (3) determining whether each subscriber has a permissible purpose. In addition, ChoicePoint alert its subscribers to the penalties for violating FCRA.

Security Program: ChoicePoint shall establish, implement and maintain a well-documented, comprehensive information security program reasonably designed to (1) protect the security, confidentiality, and integrity of consumers' personal information and (2) contain administrative, technical and physical safeguards appropriate for the size, complexity, nature, and scope of its business.

Requirements of Security Program: The program shall include:

(1) Designation of an employee responsible for the security program;

(2) Identification of internal and external threats to the security, confidentiality, and integrity of personal information through an assessment focusing on employee training, information systems, and potential system failures;

(3) Design and implement reasonable safeguards to identified risks; and

(4) Evaluation and adjustment of the information security program according to assessment and any material changes in business.

Third Party Audit: Within 180 days after service of order and thereafter biannually for twenty years, ChoicePoint must obtain an assessment and report from an independent, third party within 60 days after the end of the reporting period that:

(1) Sets forth the specific safeguards implemented and maintained by ChoicePoint;

(2) Explains how such safeguards are appropriate for the size and complexity of ChoicePoint, the nature and scope of ChoicePoint's activities and the sensitivity of the consumers' information;

(3) Explains how the implemented safeguards meet or exceed the protections required above; and

(4) Certifies that ChoicePoint's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents: For a period of six years, ChoicePoint shall create and retain the following:

(1) Subscriber files containing all materials used to verify the identity of subscribers;
(2) Consumer complaints and responses to complaints;
(3) Copies of all training materials;
(4) Copies of all subpoenas and communications with law enforcement personnel; and
(5) Copies of all records or documents that show full compliance with the order.

For a period of three years after the preparation of each biennial assessment, ChoicePoint shall retain all plans, reports, studies, reviews, audits, audit trails, policies, training materials, work papers and assessments.

Delivery of Order: For a period of five years after service of the order, ChoicePoint shall deliver a copy of the FTC order to all officers, directors, and managers who have responsibility related to this order. Within ten days after service of order, ChoicePoint shall deliver an accurate summary of the order to all current employees who are engaged in conduct related to ChoicePoint's compliance with the order or the required information security program and assessments. Future employees engaging in the above conduct should receive the summary no later than the date they assume job responsibilities. ChoicePoint shall obtain signed and dated statements acknowledging receipt of the order from each person.

Reporting: For a period of 20 years after service of the order, ChoicePoint shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Within 180 days after service of order and thereafter as requested, ChoicePoint shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: $10,000,000 in civil penalties plus an additional $5,000,000 that the FTC used to create a fund for consumer redress

The FCRA also imposes process requirements on consumer reporting agencies, companies that furnish data to the consumer reporting agencies and users of consumer reports. For example, under the Fair Credit Reporting Act, companies that use consumer reports must provide individuals with notice when information in a consumer report is used in whole or in part to make an adverse decision. The Federal Trade Commission and state attorneys general can bring actions to enforce the adverse action notice requirements of the FCRA.

THE QUICKEN LOANS CASE (DECEMBER 2002)[135]

Respondent: Quicken Loans, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violation of Fair Credit Reporting Act

Facts and Allegations: The FTC alleged that Quicken Loans, a Michigan-based mortgage lender, failed to provide consumers with adverse action notices as required by the FCRA. Section 615(a) of the FCRA requires consumers to receive an adverse action notice whenever information in a consumer report is used (in whole or in part) to make a decision adverse to the consumer, such as the denial of a loan application. The adverse action notice alerts the consumer to the fact that information in a consumer report has factored in the decision-making process and provides the consumer with the opportunity to access the consumer report and address any errors.

Outcome: Quicken Loans entered into a consent decree with the FTC, agreeing to provide consumers with notices that comply with the FCRA whenever it takes adverse actions against them. The FTC allowed Quicken Loans to restructure its online application process to allow it to avoid triggering the adverse action notice requirement: "Under the proposed order, the FTC would not view Quicken Loans' failure to grant an online request for preapproval as an adverse action if the company meets certain specific requirements, including that:

- Quicken Loans provides a clear and conspicuous disclosure in close proximity to the preapproval offer that preapproval may be granted online or offline; and
- if Quicken Loans determines it cannot grant preapproval online because it needs additional information, it notifies the consumer that: 1) the request for preapproval has not been denied, but that Quicken Loans needs additional information from the consumer; and 2) if the consumer submits the additional information, Quicken Loans will decide whether to grant the request and inform the consumer of its decision. "

Fine Imposed: None

In 2003, the FCRA was amended by the **Fair and Accurate Credit Transaction Act (FACTA)**, which added substantive new provisions to the FCRA to address identity theft and to improve the accuracy of consumer reports. For example, to help combat identity theft, FACTA revised the FCRA to provide for new classes of fraud alerts that consumers could add to their credit reports.

Because consumer reports contain Social Security numbers and other sensitive personal information, FACTA also revised the FCRA to require users of consumer reports to securely dispose of them. Pursuant to this amendment, the Federal Trade Commission has published a Disposal Rule, which sets the standards that companies using consumer reports must follow when disposing of any paper or media containing consumer reporting information. As discussed in Chapter 4, the Federal Trade Commission, like most regulators, aggressively enforces when companies fail to take appropriate measures to secure sensitive personal information.

THE AMERICAN UNITED MORTGAGE CASE (DECEMBER 2007)[136]

Respondent: American United Mortgage Company

Regulator: Federal Trade Commission

Basis for Complaint: Violation of Fair Credit Reporting Act (Disposal Rule) as well as violations of the Gramm-Leach-Bliley Act Safeguards Rule and Privacy Rule

Facts and Allegations: American United Mortgage collects sensitive personal information from and about consumers, including credit reports and sensitive financial information. The FTC complaint alleged that the company failed to implement reasonable policies and procedures to protect the sensitive information, as required by the GLBA Safeguard Rule, and to properly dispose of consumer reports, as required by the FCRA Disposal Rule. The complaint also alleged that the company failed to otherwise comply with the GLBA Privacy Rule, by not providing required consumer privacy notices.

As a result of the Safeguards Rule and Disposal Rule violations, the FTC noted that hundreds of documents containing sensitive personal information were tossed into an unsecured, easily accessible public dumpster, including 36 consumer reports.

Outcome: The settlement with the FTC requires American United Mortgage to:

(1) Comply fully with the Disposal Rule, Safeguards Rule and Privacy Rule;

(2) Obtain, every two years, for the next ten years, an audit performed by a qualified, independent third party professional to ensure that its security program meets the requirements of the order; and

(3) Pay a civil money penalty.

Fine Imposed: $50,000 for violation of the FCRA Disposal Rule

Finally, like most data protection laws, the Fair Credit Reporting Act requires entities to maintain reasonably accurate information about consumers. The Act prohibits reporting obsolete information, and requires furnishers of information to consumer reporting agencies to address any accuracy issues. In August 2000, the Federal Trade Commission announced a settlement with Performance Capital Management (PCM). The Federal Trade Commission had accused PCM of routinely reporting inaccurate information to consumer reporting agencies and refusing to investigate consumer disputes. (PCM purportedly reported incorrect delinquency dates for consumer accounts, resulting in negative information appearing incorrectly on consumer reports.) In settling the charges, PCM was enjoined from committing any further violations of the FCRA's accuracy provision and assessed a $2,000,000 penalty.[137]

Healthcare Information and Medical Records

The **Health Insurance Portability and Accountability Act of 1998 (HIPAA)** directed the Department of Health and Human Services (HHS) to promulgate privacy and security rules to govern the handling of personal information by healthcare providers, health insurance companies and healthcare clearinghouses. HHS has the authority to enforce these rules. The HHS Office of Civil Rights (OCR) enforces the HIPAA Privacy Rule, while the HHS Centers for Medicare and Medicaid Services (CMS) enforces the HIPAA Security Rule.

Although there have not yet been many high-profile HIPAA actions, both OCR and CMS have been working with companies covered by the HIPAA rules to address non-compliance.

THE HIPAA PRIVACY RULE CASES[138]

Respondent: Various companies – see details below

Regulator: Department of Health and Human Services, Office of Civil Rights

Basis for Complaint: Violations of the HIPAA Privacy Rule

Facts, Allegations and Outcomes: The following case summaries are posted on the OCR website. These reflect a sample of the OCR enforcement activities around the Privacy Rule.[139]

(1) **Inappropriate Disclosures of Protected Health Information**

- **Large Provider Revises Process to Prevent Unauthorized Disclosures to Employers**
  A state health sciences center disclosed protected health information to a complainant's employer without authorization. Among other corrective actions to resolve the specific issues in the case, including mitigation of harm to the complainant, OCR required the Center to revise its procedures regarding patient authorization prior to release of protected health information to an employer. All staff was trained on the revised procedures.

- **Public Hospital Corrects Impermissible Disclosure of Protected Health Information in Response to a Subpoena**
  A public hospital, in response to a subpoena (not accompanied by a court order), impermissibly disclosed the protected health information (PHI) of one of its patients. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order. Among other corrective actions to remedy this situation, OCR required that the hospital revise its subpoena processing procedures. Under the revised process, if a subpoena is received that does not meet the requirements of the Privacy Rule, the information is not disclosed; instead, the hospital contacts the party seeking the subpoena and the requirements of the Privacy Rule are explained. The hospital also trained relevant staff members on the new procedures.

- **Outpatient Surgical Facility Corrects Privacy Procedure in Research Recruitment**
  An outpatient surgical facility disclosed a patient's protected health information (PHI) to a research entity for recruitment purposes without the patient's authorization or an Institutional Review Board (IRB) or privacy-board-approved waiver of authorization. The outpatient facility reportedly believed that such disclosures were permitted by the Privacy Rule. OCR provided technical assistance to the covered entity regarding the requirement that covered entities seeking to disclose PHI for research recruitment purposes must obtain either a valid patient authorization or an Institutional Review Board (IRB) or privacy-board-approved alteration to or waiver of authorization. Among other corrective actions to resolve the specific issues in the case, OCR required the outpatient facility to: revise its written policies and procedures regarding disclosures of PHI for research recruitment purposes to require valid written authorizations; retrain its entire staff on the new policies and procedures; log the disclosure of the patient's PHI for accounting purposes; and send the patient a letter apologizing for the impermissible disclosure.

(2) **Safeguarding Protected Health Information**

- **Pharmacy Chain Institutes New Safeguards for Protected Health Information**
  A grocery store based pharmacy chain maintained pseudoephedrine log books containing protected health information in a manner so that individual protected health information was visible to the public at the pharmacy counter. Initially, the pharmacy chain refused to acknowledge that the log books contained protected health information. OCR issued a written analysis and a demand for compliance. Among other corrective actions to resolve the specific issues in the case, OCR required that the pharmacy chain implement national policies and procedures to safeguard the log books. Moreover, the entity was required to train of its staff on the revised policy. The chain acknowledged that log books contained protected health information and implemented the required changes.

- **Large Medicaid Plan Corrects Vulnerability that Had Resulted in Wrongful Disclosure**
  A municipal social service agency disclosed protected health information while processing Medicaid applications by sending consolidated data to computer vendors that were not business associates. Among other corrective actions to resolve the specific issues in the case, OCR required that the social service agency develop procedures for properly disclosing protected health information only to its valid business associates and to train its staff on the new processes. The new procedures were instituted in Medicaid offices and independent health care programs under the jurisdiction of the municipal social service agency.

- **Health Plan Corrects Computer Flaw that Caused Mailing of EOBs to Wrong Persons**
  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 the health plan's computer system put the protected health information of approximately 2,000 families at risk of disclosure in violation of the Rule. Among the corrective actions required to resolve this case, OCR required the insurer to correct the flaw in its computer system, review all transactions for a six month period and correct all corrupted patient information.

(3) **Respecting Rights of Access**

- **Private Practice Revises Process to Provide Access to Records**
  A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. OCR's investigation determined that the private practice had relied on state regulations that permit a covered entity to provide a summary of the record. OCR provided technical assistance to the covered entity, explaining that the Privacy Rule permits a covered entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the covered entity to revise its policy. In addition, the covered entity forwarded the complainant a complete copy of the medical record.

- **Private Practice Revises Process to Provide Access to Records**
  At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

With regard to the HIPAA Security Rule, the Centers for Medicare and Medicaid Services (CMS) has enforcement authority. CMS' published December 2007 enforcement statistics report indicates that it has considered 379 Security Rule complaints, of which 99 are still open and 280 have been resolved. Of the resolved cases, CMS reports that 49 of the cases (17.5%) were closed after corrective action was

taken.[140]

Medical records are, of course, contain some of the most sensitive types of data that exist. Outside the United States, medical information is also classified as sensitive or, in European parlance, one of the "special categories of data." Companies are generally expected to obtain consent for the processing of sensitive data. In some jurisdictions, such as Dubai International Financial Centre, a special permit must be obtained from the data protection authority before sensitive data can be processed.

In Europe, the "freely-given" consent of the individual is typically required for processing of health-related information. Data protection authorities view violations of this rule very seriously. In 2004, the Greek data protection authority fined an insurance company €20,000 for processing health data without consent. In this case, health insurance policy holders complained to the data protected authority that their health insurance company required them to consent to the disclosure and review of their health records. The Greek authority concluded that; because consent was "required," it was not "freely-given" and therefore was not adequate consent to justify the processing of the sensitive health data. Although the authority noted that the insurance company might need to process health information, it could not justify the processing by claiming that it had consent, it the consent had not been freely-given.[141]