EXAMPLES
of HIPAA violations
Minimum Necessary Policies

- Hospital Implements New Minimum Necessary Polices for Telephone Messages
- Covered Entity: General Hospital
- Issue: Minimum Necessary; Confidential Communications

A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient’s home telephone number, despite the patient’s instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. One addressed the issue of minimum necessary information in telephone message content. Employees were trained to provide only the minimum necessary information in messages, and were given specific direction as to what information could be left in a message. Employees also were trained to review registration information for patient contact directives regarding leaving messages. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.
Impermissible Uses and Disclosures; Authorizations

• HMO Revises Process to Obtain Valid Authorizations
• Covered Entity: Health Plans / HMOs
• Issue: Impermissible Uses and Disclosures; Authorizations

A complaint alleged that an HMO impermissibly disclosed a member’s PHI, when it sent her entire medical record to a disability insurance company without her authorization. An OCR investigation indicated that the form the HMO relied on to make the disclosure was not a valid authorization under the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, the HMO created a new HIPAA-compliant authorization form and implemented a new policy that directs staff to obtain patient signatures on these forms before responding to any disclosure requests, even if patients bring in their own “authorization” form. The new authorization specifies what records and/or portions of the files will be disclosed and the respective authorization will be kept in the patient’s record, together with the disclosed information.
Improper Charges for Medical Record Copies

• Entity Rescinds Improper Charges for Medical Record Copies to Reflect Reasonable, Cost-Based Fees
  Covered Entity: Private Practice
  Issue: Access

• A patient alleged that a covered entity failed to provide him access to his medical records. After OCR notified the entity of the allegation, the entity released the complainant’s medical records but also billed him $100.00 for a “records review fee” as well as an administrative fee. The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. To resolve this matter, the covered entity refunded the $100.00 “records review fee.”
Safeguards; Impermissible Uses and Disclosures

- **Private Practice Implements Safeguards for Waiting Rooms**
  
  **Covered Entity:** Private Practice
  
  **Issue:** Safeguards; Impermissible Uses and Disclosures

- A staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals. Also, computer screens displaying patient information were easily visible to patients. Among other corrective actions to resolve the specific issues in the case, OCR required the provider to develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI. The practice trained all staff on the newly developed policies and procedures. In addition, OCR required the practice to reposition its computer monitors to prevent patients from viewing information on the screens, and the practice installed computer monitor privacy screens to prevent impermissible disclosures.
Impermissible Uses and Disclosures; Business Associates

• **Pharmacy Chain Enters into Business Associate Agreement with Law Firm**
  
  Covered Entity: Pharmacy Chain  
  Issue: Impermissible Uses and Disclosures; Business Associates

• A complaint alleged that a law firm working on behalf of a pharmacy chain in an administrative proceeding impermissibly disclosed the PHI of a customer of the pharmacy chain. OCR investigated the allegation and found no evidence that the law firm had impermissibly disclosed the customer’s PHI. However, the investigation revealed that the pharmacy chain and the law firm had not entered into a Business Associate Agreement, as required by the Privacy Rule to ensure that PHI is appropriately safeguarded. Without a properly executed agreement, a covered entity may not disclose PHI to its law firm. To resolve the matter, OCR required the pharmacy chain and the law firm to enter into a business associate agreement.
Impermissible Uses and Disclosures

- **Radiologist Revises Process for Workers Compensation Disclosures**
  
  Covered Entity: Health Care Provider
  
  Issue: Impermissible Uses and Disclosures

- A radiology practice that interpreted a hospital patient’s imaging tests submitted a worker’s compensation claim to the patient’s employer. The claim included the patient’s test results. However, the patient was not covered by worker’s compensation and had not identified worker’s compensation as responsible for payment. OCR’s investigation revealed that the radiology practice had relied upon incorrect billing information from the treating hospital in submitting the claim. Among other corrective actions to resolve the specific issues in the case, the practice apologized to the patient and sanctioned the employee responsible for the incident; trained all billing and coding staff on appropriate insurance claims submission; and revised its policies and procedures to require a specific request from worker’s compensation carriers before submitting test results to them.
Safeguards

• Health Plan Corrects Computer Flaw that Caused Mailing of EOBs to Wrong Persons
  Covered Entity: Health Plans
  Issue: Safeguards

• 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.
Impermissible Disclosure; Confidential Communications

• Large Provider Revises Patient Contact Process to Reflect Requests for Confidential Communications
  Covered Entity: General Hospital
  Issue: Impermissible Disclosure; Confidential Communications

• A patient alleged that a general hospital disclosed protected health information when a hospital staff person left a message on the patient’s home phone answering machine, thereby failing to accommodate the patient’s request that communications of PHI be made only through her mobile or work phones. In response, the hospital instituted a number of actions to achieve compliance with the Privacy Rule. To resolve this matter to the satisfaction of OCR, the hospital: retrained an entire Department with regard to the requirements of the Privacy Rule; provided additional specific training to staff members whose job duties included leaving messages for patients; and, revised the Department’s patient privacy policy to clarify patient rights to accommodation of reasonable requests to receive communications of PHI by alternative means or at alternative locations.
Impermissible Use

• Large Health System Restricts Provider's Use of Patient Records
  Covered Entity: Multi-Hospital Healthcare Provider
  Issue: Impermissible Use

• A nurse practitioner who has privileges at a multi-hospital health care system and who is part of the system’s organized health care arrangement impermissibly accessed the medical records of her ex-husband. In order to resolve this matter to OCR’s satisfaction and to prevent a recurrence, the covered entity: terminated the nurse practitioner’s access to its electronic records system; reported the nurse practitioner’s conduct to the appropriate licensing authority; and, provided the nurse practitioner with remedial Privacy Rule training.
Access

- **Private Practice Revises Access Procedure to Provide Access Despite an Outstanding Balance**
  Covered Entity: Private Practice
  Issue: Access

- A complainant alleged that a private practice physician denied her access to her medical records, because the complainant had an outstanding balance for services the physician had provided. During OCR’s investigation, the physician confirmed that the complainant was not given access to her medical record because of the outstanding balance. OCR provided technical assistance to the physician, explaining that, in general, the Privacy Rule requires that a covered entity provide an individual access to their medical record within 30 days of a request, regardless of whether or not the individual has a balance due. Once the physician learned that he could not withhold access until payment was made, the physician provided the complainant a copy of her medical record.
Conditioning Compliance with the Privacy Rule

- **Private Practice Ceases Conditioning of Compliance with the Privacy Rule**
  
  **Covered Entity:** Private Practice  
  **Issue:** Conditioning Compliance with the Privacy Rule

- A physician practice requested that patients sign an agreement entitled “Consent and Mutual Agreement to Maintain Privacy.” The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/or treatment in exchange for the physician’s compliance with the Privacy Rule. A patient’s rights under the Privacy Rule are not contingent on the patient’s agreement with a covered entity. A covered entity’s obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient’s silence. OCR required the covered entity to cease using the patient agreement that conditioned the entity’s compliance with the Privacy Rule. Additionally, OCR required the covered entity to revise its Notice of Privacy Practices.
Access

• Private Practice Revises Process to Provide Access to Records Regardless of Payment Source
Covered Entity: Private Practices
Issue: Access

• 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.
Impermissible Uses and Disclosures; Authorizations

• Health Sciences Center Revises Process to Prevent Unauthorized Disclosures to Employers
  Covered Entity: General Hospitals
  Issue: Impermissible Uses and Disclosures; Authorizations

• 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.
Access

- **Private Practice Revises Process to Provide Access to Records**
  Covered Entity: Private Practices
  Issue: Access

- 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.
Impermissible Uses and Disclosures (Subpoenas)

• Public Hospital Corrects Impermissible Disclosure of PHI in Response to a Subpoena
  Covered Entity: General Hospital
  Issue: Impermissible Uses and Disclosures

• 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.
Impermissible Use and Disclosure

- **Clinic Sanctions Supervisor for Accessing Employee Medical Record**
  Covered Entity: Outpatient Facility
  Issue: Impermissible Use and Disclosure

- A hospital employee's supervisor accessed, examined, and disclosed an employee's medical record. OCR's investigation confirmed that the use and disclosure of protected health information by the supervisor was not authorized by the employee and was not otherwise permitted by the Privacy Rule. An employee's medical record is protected by the Privacy Rule, even though employment records held by a covered entity in its role as employer are not. Among other corrective actions to resolve the specific issues in the case, a letter of reprimand was placed in the supervisor's personnel file and the supervisor received additional training about the Privacy Rule. Further, the covered entity counseled the supervisor about appropriate use of the medical information of a subordinate.
Access

- **Private Practice Provides Access to All Records, Regardless of Source**
  Covered Entity: Private Practice
  Issue: Access

- A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. While the amendment provisions of the Privacy Rule permit a covered entity to deny an individual's request for an amendment when the covered entity did not create that portion of the record subject to the request for amendment, no similar provision limits individuals' rights to access their protected health information. Among other steps to resolve the specific issue in this case, OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their record regardless of whether another entity created information contained within it.
Safeguards

• **Physician Revises Faxing Procedures to Safeguard PHI**
  Covered Entity: Health Care Provider
  Issue: Safeguards

• A doctor's office disclosed a patient's HIV status when the office mistakenly faxed medical records to the patient's place of employment instead of to the patient's new health care provider. The employee responsible for the disclosure received a written disciplinary warning, and both the employee and the physician apologized to the patient. To resolve this matter, OCR also required the practice to revise the office's fax cover page to underscore a confidential communication for the intended recipient. The office informed all its employees of the incident and counseled staff on proper faxing procedures.