

How OCR Enforces the HIPAA Privacy Rule

OCR is responsible for enforcing the HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164, Subparts A, C, and E). One of the ways that OCR carries out this responsibility is to investigate [complaints](#) filed with it. OCR may also conduct compliance reviews to determine if covered entities are in compliance, and OCR performs education and outreach to foster compliance with requirements of the Privacy and Security Rules.

OCR may only take action on certain complaints. See [What OCR Considers During Intake and Review of a Complaint](#) for a description of the types of cases in which OCR cannot take an enforcement action.

If OCR accepts a complaint for investigation, OCR will notify the person who filed the complaint and the covered entity named in it. Then the complainant and the covered entity are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts. Covered entities are required by law to cooperate with complaint investigations.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to the Department of Justice for investigation.

OCR reviews the information, or evidence, that it gathers in each case. In some cases, it may determine that the covered entity did not violate the requirements of the Privacy or Security Rule. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:

- Voluntary compliance;
- Corrective action; and/or
- Resolution agreement.

Most Privacy and Security Rule investigations are concluded to the satisfaction of OCR through these types of resolutions. OCR notifies the person who filed the complaint and the covered entity in writing of the resolution result.

If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties (CMPs) on the covered entity. If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case. Complainants do not receive a portion of CMPs collected from covered entities; the penalties are deposited in the U.S. Treasury.

Source: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html>

What OCR Considers During Intake & Review

What OCR Considers During Intake & Review of a Complaint

The Office for Civil Rights (OCR) is the agency within the U. S. Department of Health and Human Services that investigates complaints about failures to protect the privacy of health information. It does so under its authority to enforce the Privacy and Security Rules.

OCR carefully reviews all complaints that it receives. Under the law, OCR only may take action on complaints that meet the following conditions.

- **The alleged action must have taken place after the dates the Rules took effect.** Compliance with the Privacy Rule was not required until April 14, 2003. Compliance with the Security Rule was not required until April 20, 2005. Therefore, OCR can not investigate complaints about actions that took place before these dates.
- **The complaint must be filed against an entity that is required by law to comply with the Privacy and Security Rules.** Not all organizations are covered by the Privacy and Security Rules. Entities subject to the Privacy and Security Rules are considered “covered entities.” Briefly, a covered entity is:
 - a health plan:
including but not limited to
 - health insurance companies,
 - company health plans; or
 - a health care provider that electronically transmits any health information in connection with certain financial and administrative transactions (such as electronically billing insurance carriers for services): including but not limited to
 - doctors,
 - clinics,
 - hospitals,
 - psychologists,
 - chiropractors,
 - nursing homes,
 - pharmacies, and
 - dentists; or
 - a health care clearinghouse.
 - **Examples of organizations that are not required to comply** with the Privacy and Security Rules include
 - life insurers,
 - employers,
 - workers compensation carriers,
 - many schools and school districts,
 - many state agencies like child protective service agencies,
 - many law enforcement agencies,

- many municipal offices
- A complaint must **allege an activity that, if proven true, would violate the Privacy or Security Rule**. For example, OCR generally could not investigate a complaint that alleged that a physician sent a person's demographic information to an insurance company to obtain payment, because the Privacy Rule generally permits doctors to use and disclose such information to bill for their services.
- Complaints **must be filed within 180 days** of when the person submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule. OCR may waive this time limit if it determines that the person submitting the complaint shows good cause for not submitting the complaint within the 180 day time frame (e.g., such as circumstances that made submitting the complaint within 180 days impossible).

Source: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/whatocrconsiders.html>

