

For Covered Entities

The Privacy and Security Rules apply only to **covered entities**. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If an entity is not a covered entity, it does not have to comply with the Privacy Rule or the Security Rule.

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
<p>This includes providers such as:</p> <ul style="list-style-type: none">• Doctors• Clinics• Psychologists• Dentists• Chiropractors• Nursing Homes• Pharmacies <p>...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.</p>	<p>This includes:</p> <ul style="list-style-type: none">• Health insurance companies• HMOs• Company health plans• Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	<p>This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.</p>

Are You a Covered Entity?

[View](#) an easy-to-use question and answer decision tool.

Guidance Materials for Small Providers, Small Health Plans, and other Small Businesses

[View materials](#) about the Privacy Rule for small providers, small health plans and other small

businesses.

Guidance Materials for Covered Entities

[Summary of the Privacy Rule](#)-This is a summary of the key elements of the Privacy Rule, including who is covered, what information is protected, and how covered entities can use and disclose protected health information.

[Guidance on Significant Aspects of the Privacy Rule](#)-A collection of documents explaining many provisions of the Privacy Rule including business associates, special topics such as disclosures for public health and research, and incidental uses and disclosures.

[Summary of the Security Rule](#)-This is a summary of the key elements of the Security Rule, including what administrative, physical, and technical safeguards covered entities must have in place to protect the security of electronic protected health information.

[Guidance on How to Comply with the Security Rule](#)-A collection of documents explaining how the Department expects covered entities to achieve substantial compliance with the Security Rule.

[Security Risks to Electronic Health Information from Peer-to-Peer File Sharing Applications](#)-The Federal Trade Commission (FTC) has developed a guide to Peer-to-Peer (P2P) security issues for businesses that collect and store sensitive information.

[Safeguarding Electronic Protected Health Information on Digital Copiers](#)-The Federal Trade Commission (FTC) has tips on how to safeguard sensitive data stored on the hard drives of digital copiers.

[Workshop on the HIPAA Privacy Rule's De-Identification Standard](#) - Washington, DC - March 8th & 9th, 2010

[Fast Facts for Covered Entities](#)-Answers to many common questions and misconceptions about patient consent, incidental disclosures, child abuse reporting, electronic media, and other disclosures.

[Provider Guide: Communicating With a Patient's Family, Friends, or Other Persons Identified by the Patient](#)-This is a guide for health care providers to help them determine when they can disclose a patient's health information to the patient's family, friends, or other identified by the patient.

[Guidance on the Application of FERPA and HIPAA to Student Health Records](#)-This guide addresses school administrators, health care professionals, and others

interested in how these two laws apply to student health records.

Frequently Asked Questions About Family Medical History Information-These frequently asked questions and answers address how the Privacy Rule permits the use and disclosure of medical history information.

Frequently Asked Questions About the Disposal of Protected Health Information-The frequently asked questions and answers address how covered entities should dispose of health information pursuant to the Privacy and Security Rules.

Sample Business Associate Contract-This sample contract provides covered entities with language to help them comply with the business associate requirements of the Privacy

Misleading Marketing Claims-This notice addresses marketing claims that suggest compliance programs may be endorsed by HHS. HHS and OCR do not endorse any private consultants' or education providers' seminars, materials or systems, and do not certify any persons or products as Privacy Rule compliant.

Designation of Regional Privacy Advisors-The HITECH Act requires the Secretary to designate an individual in each regional office of HHS to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to the HIPAA Privacy and Security Rules.

Sign Up for the OCR Privacy Listserv-OCR has established a listserv to inform the public about Privacy and Security Rule FAQs, guidance, and technical assistance materials as they are released.

Source: OCR's website: For Covered Entities

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>