

HIPAA

*from the United States Department of Health & Human Services Summary
of the HIPAA Privacy Rule*

The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Privacy Rule standards address the use and disclosure of individuals’ health information---called “protected health information” by the organizations who are subject to the Privacy Rule---as well as standards for individuals’ privacy rights to understand and control how their health information is used.

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide.

What information is protected?

The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information.”

“Individually identifiable health information” is information including demographic data that relates to: the individual’s past, present, or future physical or mental health condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

General Principle for Uses and Disclosures

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

Psychotherapy Notes

A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

- The covered entity who originated the notes may use them for treatment
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rule, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner, or as required by law.

Notice and Other Individual Rights

Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe the individual's rights including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making

3

complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.