## DEFINITIONS

PRIVACY RULE (2002) is a set of national standards for the protection of individually identifiable health information by three covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance was required by April 2003.

SECURITY RULE (2006) is a set of national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 2005 (April 20, 2006 for small health plans).

ENDFORCEMENT RULE is a set of standards for the enforcement of all the Administrative Simplification Rules.

FINAL OMNIBUS RULE implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

BREACH NOTIFICATION RULE. An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

HITECH ACT is the Health Information Technology for Economic and Clinical Health Act, a part of the American Recovery and Reinvestment Act of 2009, intended to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RECORD is a term that means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

## FREQUENTLY ASKED QUESTIONS

### What are the rights of patients under HIPAA?

HIPAA provides patients with the right over their own health information including:

- Receiving a copy of it;
- Being permitted to make corrections to it;
- Learning how health information is used and shared;
- Informing providers or health insurance companies if there is information that is not to be shared;
- Requesting to be reached somewhere other than home.

### What is included in the HIPAA Privacy Notice?

The notice explains to patients how their health information can be used or shared. A copy is provided to patients at their first appointment or when enrolling in a new health plan and is posted in a visible location. The notice should include the following:

- How the health care provider or insurer is allowed to use or share health information;
- The patient's privacy rights, including the right to be provided with a copy of their health file, to review it;
- Inform the patient that their medical file may corrected;
- The right to file a complaint if the patient believes their privacy rights have been violated;
- The doctor or insurer's legal duties to protect health information;
- Who to contact for more information about the health provider or insurance company's privacy policies.

### What happens if a patient wants to share health information with a family member or a friend?

HIPAA requires health care providers to protect the privacy of medical information. Patients may request that certain information be disclosed to family members or friends under certain circumstances. This may occur when the patient is present or not present, and requires the professional judgment of the provider in consideration of the well-being of the patient.

A few scenarios are:

- An emergency room doctor may discuss a patient's treatment in front of a family member when they are present in the treatment room at the request of the patient.
- A doctor may not discuss the patient's health condition with any family member if the patient tells him or her not to.
- HIPAA also permits health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person that the patient has requested to pick up.

**What is a covered entity required to do at the minimum to protect a patient's health information?**

A covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. A covered entity also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs. However, covered entities are not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes.