Chapter 1

Welcome to HIPAA

If this is your first time exploring health care privacy and security, welcome to this important area of health law. Just about every aspect of health care has been affected by the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In fact, members of the public seem to use the term “HIPAA” as a kind of shorthand for all types of health privacy. HIPAA is intended to make it easier for individuals to obtain copies of their own health records and much more difficult for others to disclose this information. HIPAA imposes many responsibilities on health care providers and their business associates and it casts a wide net. From hospitals to doctors’ offices to school health clinics, the HIPAA Privacy and Security Rules have transformed the way health care providers and others handle health records. The Privacy, Security, and Enforcement Rules are the most commonly referenced sections of HIPAA. But there are other portions of HIPAA that are often overlooked. Whether this is your first time examining HIPAA or you are a pro looking for a refresher, this book is intended to provide you with the HIPAA basics as well as updates that have come about since the first edition. This first chapter will provide an overview of the various components...
of the federal law known as HIPAA. HIPAA is divided into five titles, which are briefly explained in the following subsections.

I. Title I

HIPAA, passed in 1996, also known as the Kennedy-Kassebaum Act, was designed to promote the availability of health care as well as administrative simplification. Title I: Health Care Access, Portability, and Renewability protects workers’ health insurance when employees change or lose their jobs and prohibits group health insurers from excluding or discriminating against individuals who have preexisting health conditions. It requires employers and health plans to allow a new employee’s medical insurance coverage to continue regardless of whether he or she have had a preexisting condition.

Title I imposes certain restrictions on health insurers when they decide not to renew or to discontinue coverage. A health insurer may discontinue health insurance coverage in the group or individual market only for: (1) nonpayment of premiums; (2) fraud; (3) violation of participation rules; (4) termination of product; (5) enrollee’s movement outside of service area; or (6) if the employer’s membership stops.1 As stated above, Title I protects workers and their families from being denied health insurance coverage when the worker changes jobs or loses his or her job, which makes health insurance coverage “portable.” But make no mistake, Title I does not require the same health insurance company to provide benefits when the employee changes jobs. Rather, it prevents a worker and his or her family from being denied coverage when the worker is no longer associated with that particular job.2 For example, if an employee’s wife develops cancer and sometime

---

later the employee leaves that employer to become employed at a different company, the new employer’s health insurance company cannot deny coverage to the new employee’s family (including the wife), despite the wife’s previous existing cancer diagnosis. We take this for granted now and many of us have never known anything different, but there was a time in America when health insurance companies could routinely deny coverage due to a preexisting health condition. Previous to HIPAA, if someone in the family had a chronic or long-lasting health condition such as diabetes or depression, the worker whose job provided health care insurance coverage was obligated to stay at his or her job in order to maintain health insurance coverage for the family.

II. Title II

The next section of HIPAA is Title II, which is the section with which most people are familiar. Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform is also known as the Administrative Simplification Rule. Title II permits the U.S. Department of Health and Human Services to create standards for electronic health care transactions made by health care providers, health plans, and employers, which includes the security and privacy of health information. This book focuses on the Privacy and Security sections of the Administrative Simplification Rules and are explained in detail throughout the book. Title II contains the HIPAA Privacy, Security, and Enforcement portions as well as the Transactions and Codes Set Standards and the Identifier Standards for Employers and Providers.\(^3\) The intent of Title II is to improve the efficiency and effectiveness of the nation’s health care system by encouraging the widespread

---

use of electronic data interchange in health care. In creating provisions for the electronic transfer of health information, Congress recognized that safeguards were needed to control the exchange of highly personal and confidential medical information. The standards are meant to improve the efficiency and effectiveness of the nation’s health care system by encouraging the widespread use of electronic data interchange in health care.

Title II is also meant to reduce the costs and administrative burdens of health care by standardizing the electronic transmission of certain administrative and financial transactions that had been previously done on paper. In its quest to restrain health care costs, the government determined that a high percentage of every health care dollar spent was on administrative overhead, including processing for enrollment, payment, eligibility, authorizations, filing a claim, supporting a claim, coordinating payments between more than one insurance company, and notifying the provider about payment. In order to rein in costs, the Administrative Simplification Rule was put in place.

This book specifically explains the Privacy, Security, and Enforcement Rules and provides practical information on implementation and compliance. There are three primary types of entities that are covered under HIPAA: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. These types of entities that are covered by HIPAA are referred to as “covered entities.” As discussed ahead, HIPAA has now been expanded to directly govern business associates of covered entities, as well as their subcontractors.

The final Privacy Rule was published in December of 2000 and later modified in August 2002. As the name implies, the Privacy

4. Id.
6. 45 C.F.R. § 160.103.
Chapter 1: Welcome to HIPAA

Rule sets national standards for the protection of individually identifiable health information. Covered entities were required to comply with the Privacy Rule as of April 14, 2003 (April 14, 2004, for small health plans). The Privacy Rule is codified at 45 C.F.R. Part 164, Subparts A & E.

The final Security Rule was published in February of 2003. The Security Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Covered entities were required to comply with the Security Rule as of April 20, 2005 (April 20, 2006, for small health plans). The Security Rule is codified at 45 C.F.R. Part 160 and Subparts A and C of Part 164. It requires covered entities to provide appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. More details about the Security Rule can be found in Chapter 6.

The Enforcement Rule provides standards for enforcing HIPAA and was published in February of 2006. It contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 C.F.R. Part 160, Subparts C, D, and E.

Other rules also affect electronic data use in health care and somewhat enhance Title II. For example, as part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act became effective on February 18, 2009. The HITECH Act, discussed in more detail in Chapter 7, is intended to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act contains several provisions that strengthen the civil and criminal enforcement of the privacy and security rules associated with electronic transmission of health information. The HITECH Act gave individuals the right to be notified of breaches, expanded HIPAA’s reach to business associates, and increased penalties.
The interim final rule relating to breach notification for unsecured protected health information, implementing portions of the HITECH Act, was published in August of 2009. A final breach rule, also referred to as the omnibus rule, was published in January of 2013 and implements a number of provisions of the HITECH Act.

Another rule that implicates Title II is the Patient Protection and Affordable Care Act (ACA), 42 U.S.C. 18001, Pub. L. No. 111-148, which went into effect on January 7, 2011. The ACA expanded the Administrative Simplification provisions of HIPAA Title II and introduced operating rules to standardize business practices. These operating rules contain certain requirements for transactions under HIPAA that specify the information that must be included when conducting standard transactions. This book includes information about the HITECH Act and the ACA in the discussion about HIPAA Title II.


III. Title III

Title III contains the tax-related health provisions of HIPAA. These provisions mostly relate to one of two major topics: medical savings accounts (MSAs) or long-term care. MSAs are the predecessors of health savings accounts (HSAs). MSAs were a federal pilot