CHAPTER 1

Introduction

Data security breaches are an everyday occurrence. The news media constantly publicize data breaches, especially those involving retailers in which hackers steal the payment card information from millions of consumers. Perhaps of more concern, though, are data breaches in the healthcare field.

In February 2015, Anthem, Inc., the country’s second-largest health insurer, announced a massive data breach involving unauthorized access to its database of personal information concerning current and former Anthem members. Victims around the country have experienced identity theft incidents. At the time of this writing, a class action pending in the US District Court for the Northern District of California now seeks compensation for the victims. Also, from 2004 to 2008, former California First Lady Maria Shriver, the late actress Farrah Fawcett, singer Britney Spears, and Cheers actress Shelley Long were all victims of breaches involving the unauthorized access to their medical records at the UCLA Medical Center. In the past several months, news reports surfaced regarding hospitals that have fallen victim to “ransomware” attacks. Ransomware is a form of malicious software that, when it infects a computer system, quickly encrypts data on the system and sometimes network storage or other computers. The victim receives a message demanding ransom money to provide a key to decrypt the user’s files. If the user fails to pay the ransom, the user could lose access to his or her data. Recent ransomware attacks have locked up electronic medical records of entire hospitals, disabling their information systems and potentially endangering patients.

Health records are among the most sensitive sets of information about us. The results of an unauthorized disclosure of health records could be devastating. Leakage of health records could lead to victims’ embarrassment, stigma, job loss, and even identity theft. Following concerns about the privacy and security of health records in the 1990s, the public began to demand protection to ensure that the healthcare industry would implement controls over what information was
gathered from patients, how the information could be shared, and the secure management of that information. This public concern prompted Congress to enact legislation in 1996 calling for safeguards over the privacy and security of health information.

The 1996 legislation, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has had a broad impact on the healthcare industry since its enactment, transforming practices for creating, storing, managing, transmitting, and disclosing health information in this country. HIPAA called for federal standards for the privacy and security of certain health information (called protected health information under HIPAA, and PHI here). The privacy and security portions of HIPAA appear in the Administrative Simplification subtitle of HIPAA, and later regulations create the standards for privacy and security. The Department of Health and Human Services (HHS) promulgated these regulations in the form of a Privacy Rule and a Security Rule.

In general, HHS intended the administrative simplification provisions in HIPAA to increase the ease and efficiency of exchanging health information and conducting healthcare transactions electronically. Specifically, HIPAA contemplated the use of electronic data interchange (EDI) to accelerate electronic processing of transactions in the healthcare industry. HHS hoped standardizing the formats for many of the most common EDI exchanges of health information would mean the end of much of the confusion in claims submission and payment caused by inconsistent formats and forms, under the Medicare and Medicaid Programs, and beyond. Since the enactment of HIPAA, the healthcare field has seen the proliferation of Internet-based services and cloud computing in addition to EDI. Nonetheless, the Privacy Rule and Security Rule have continued to govern the creation, receipt, use, processing, maintenance, and transmission of electronic PHI regardless of the technology used by businesses in the healthcare field.

The American Bar Association Section of Science & Technology Law published the first edition of this book in 2007. Since then, two important sets of changes to the law have taken place. First, Congress

---

Introduction

passed the Health Information Technology for Economic and Clinical Health Act, also called the HITECH Act. The HITECH Act is part of a larger piece of stimulus legislation enacted during the financial crisis that started in the late 2000s. The HITECH Act made certain changes to HIPAA security and privacy provisions, called for notification of data security breaches to affected individuals, and strengthened HIPAA’s enforcement provisions.

Second, HHS issued interim and later final regulations to flesh out the provisions of the HITECH Act, to strengthen HIPAA enforcement, and to somewhat simplify the HIPAA Security Rule and the HIPAA Privacy Rule. The final set of regulations emerging from the HITECH Act is commonly referred to as the HIPAA Final Omnibus Rule. The compliance deadline for the HIPAA Final Omnibus Rule was in September 2013.

Unlike other books on HIPAA, the focus of this book is the HIPAA Security Rule, as modified by the HITECH Act and the HIPAA Final Omnibus Rule. This publication discusses the Security Rule’s role in the broader context of HIPAA, the HITECH Act, and their regulations. At the heart of this publication is a detailed section-by-section analysis of each provision in the Security Rule covering a security safeguard. This analysis explains the security topic and what organizations can do to comply. This publication also covers the legal risks of noncompliance by describing the applicable enforcement mechanisms that apply, reporting on past enforcement actions, and describing the body of case law emerging from litigation relating to HIPAA/HITECH security. The intended audience of this book is healthcare and information security professionals, lawyers specializing in these fields, administrators, compliance officers, chief information security officers, and security personnel. Hopefully, the book will provide the reader with useful guidance in meeting security requirements related to PHI.

The Security Rule focuses on PHI in electronic form. The HIPAA Privacy Rule also requires covered entities to implement “appropriate administrative, technical and physical safeguards” for the privacy of PHI,

in all its forms, including paper records. At a highlevel, The safeguards described in the Privacy Rule are the same as those in the security Rule: administrative, technical, and physical safeguards. They also seek to protect PHI against unauthorized use or disclosure, as the Security Rule does.

Specifically, the Security Rule is designed to protect the confidentiality, integrity, and availability of electronic protected health information. In the first edition, we emphasized the difference between PHI addressed in the Privacy Rule by using “ePHI” for electronic PHI, which is specifically addressed in the Security Rule. In this edition, we have decided to abandon the use of “ePHI” in favor of the more commonly used generic term, PHI, because as a practical matter, HIPAA entities need to protect PHI in whatever form, and from an information security perspective, most readers will understand that the type of PHI discussed in this book is electronic PHI. This is also the approach taken in most business associate agreements.

The Security Rule requires entities covered by HIPAA (i.e., covered entities) to implement reasonable and appropriate administrative, physical, and technical safeguards to protect PHI. The HITECH Act and the HIPAA Final Omnibus Rule apply the Security Rule to “business associates” of covered entities, which perform HIPAA-covered functions on behalf of their covered entity customers or clients. Moreover, the HIPAA Final Omnibus Rule covers a broad range of technology vendors and service providers, many of which may offer general-purpose services, may have no intention of focusing on the healthcare market, and may even be unaware that their customers are using their services to store PHI on their systems. Accordingly, the breadth of the HIPAA Final Omnibus Rule has been a surprise to many vendors and service providers.

HIPAA/HITECH safeguards must secure PHI while in the custody of covered entities and business associates, as well as during transmission to or from these businesses. Such safeguards must be adequate to ensure the confidentiality of the information. They must also protect against any reasonably anticipated threats or hazards to the security and integrity of the PHI and protect against unauthorized use or disclosure of the PHI.

Assessing and managing risks are the primary challenges posed by HIPAA security compliance. Risk assessment is the first step in identifying the security threats and hazards that a given covered entity or business

6. 45 C.F.R. § 164.530(c)(i).
7. Compare id. § 164.530(c)(2)(i) to id. § 164.306(a)(3).
8. Covered entities are health plans, healthcare providers, and healthcare clearinghouses. 45 C.F.R. § 160.103.
associate can reasonably anticipate, as well as the costs that will be reasonable and appropriate in addressing those risks. Risk assessment includes prioritizing and quantifying the risks. Mitigation and remediating threats that pose risks should follow the risk assessment. If mitigation and remediation are not reasonable and appropriate, it may be necessary to transfer risks (using insurance or third-party indemnification, for instance) or to simply accept and plan on handling risks that cannot otherwise be mitigated. Regardless, the Security Rule requires ongoing monitoring and periodic review to facilitate an ongoing assessment and reevaluation of risks.

Secure electronic transmission of health information offers opportunities to improve the quality and efficiency of healthcare delivery by improving access to information. Specifically, access by healthcare professionals, health plan administrators, and patients will improve. In addition, secure transmission of electronic health information will foster opportunities to implement cost savings as a result of standardized healthcare transactions and the use of the Internet and cloud service providers. Secure electronic transmission of health information can create opportunities to identify and treat those who are at risk for specific diseases, to conduct medical research, and to detect fraud and abuse.

Moreover, the distribution of electronic data can extend far beyond the community where the patient is physically located. Prior to the promulgation of national standards for the confidentiality, security, and electronic exchange of PHI, disparate state laws were a source of confusion and inconsistency. By contrast, comprehensive minimum national standards\(^9\) for the privacy and security of PHI will encourage increased and appropriate use of electronic information while protecting a patient’s need for privacy.\(^{10}\)

Another important health information trend has been the proliferation of non-PC mobile devices. Electronic health data is becoming increasingly mobile as more information becomes available in electronic form. Since the first edition of this book, a revolution in mobile computing has taken place, and mobile computing holds the promise

---

9. HIPAA does not establish comprehensive standards. Rather, it sets a national uniform “floor” of standards. HIPAA expressly preserves state privacy laws that are in conflict with HIPAA if the state provision is “more stringent” than the federal provisions. 45 C.F.R. § 160.203. Consequently, there could potentially be different versions of privacy rules for each of the states, the District of Columbia, Puerto Rico, and U.S. possessions and territories.

10. State laws requiring the protection of personal information of citizens are becoming increasingly common. One example is California’s AB 1950. Cal. Civil Code § 1798.81.5. AB 1950, however, does not apply to covered entities, perhaps to avoid disturbing the national standard created by the Security Rule. Id. § 1798.81.5(e)(3).
for significant changes in the way professionals provide healthcare services. Healthcare professionals are commonly using smartphones and tablet computers for their everyday work. In addition, special hardware and software applications allow healthcare professionals and patients to use their general-purpose mobile devices for a wide variety of diagnostic, imaging, and wellness applications. Covered entities and business associates must now account for mobile computing in their Security Rule and Privacy Rule compliance programs. Managing mobile health initiatives will not be easy, and mobile devices raise a host of general and healthcare-specific legal issues.11

Emerging technologies will pose even greater HIPAA security challenges. For instance, smart devices, wearable computers, Internet of Things devices and systems, augmented and virtual reality systems, telemedicine, 3D printing, new types of mobile devices (even automobiles), and surgical and service robots may create, receive, maintain, or transmit PHI. Covered entities and business associates will need to secure PHI on these new kinds of devices as well. Future decades will see far greater security challenges in the healthcare field. Accordingly, organizations should continuously anticipate future security threats and opportunities as they adopt emerging technologies. Hopefully, this book will assist in those efforts.

11. Author Stephen Wu has also written on the general legal issues concerning mobile device management in his August 2013 book, *A Legal Guide to Enterprise Mobile Device Management: Managing Bring Your Own Device (BYOD) and Employer-Issued Device Programs*, also published by the American Bar Association Section of Science & Technology Law.