5 Payor Privacy Issues

By Jennifer M. O'Brien, JD, CHC, CHPC

Introduction

There are great challenges in managing privacy compliance risks for all health care businesses. In fact, data privacy and security are significant issues in virtually every deal or decision made by large and small health care companies across the nation. While the requirements of the privacy laws are typically the same regardless of whether the company operates as a hospital, clinic, health plan, or sells durable medical equipment, the challenges and risk differ.

This chapter focuses on privacy issues for Covered Entity health plans. The objectives of the chapter are: 1) to provide a better understanding of basic consumer privacy issues related to health plans; 2) to provide an overview of payor privacy issues and the proper collection, use, and disclosure of consumer information; and 3) considerations related to marketing and health plan communication of products and services.

Privacy compliance in a payor world requires more of a focus on payment and operations versus the treatment issues that are more prevalent in hospital and clinic settings. Such functions include areas such as explanation of benefits (EOBs) and claims data submission. There is also an intense focus on database information and the appropriate use, collection and disclosure of information. An example of typical payor concerns might be looking at the advantage of an all-payor database and the benefit of bringing transparency to the health care market and balancing that with the increased privacy risks and concerns of consumers.
Additional focus areas within the payor world include the need to have solid processes around written or verbal consent since there is less face-to-face interaction with consumers as compared to a provider setting. As a result, verifying the identity of a consumer is important to ensure that the appropriate information is shared with the appropriate person. There are also a number of marketing considerations that a health plan needs to be aware of related to value-added services. And finally, the volume and quantity of claims processed every day is very high. As a result, an inadvertent error can potentially trigger burdensome and mandatory consumer, customer and regulatory notification obligations.

**Background**

The focus on privacy rights and the call for more stringent laws has increased with the advance of technology. The result has been the adoption of a number of federal and state laws, industry commitments and an increased consumer expectation that information will be appropriately safeguarded.

Organizations are struggling to balance business goals with legal and regulatory requirements. The balance lies between the drive to more sophisticated use of data to provide better health care services with the fast-paced regulatory effort to restrict use and disclosure of data. For health plans, greater and more sophisticated use of data is a priority as the competition increases for market share. Consumers and beneficiaries are asking for more personalized health care services and wanting electronic access to their health records, yet legislative and enforcement activity is focusing on more stringent regulatory oversight.

The increased consumer and regulatory focus has resulted in greater attention given to ensure appropriate resources are in place to support privacy compliance efforts. It is important that a health plan develop a practical approach to safeguarding the privacy of information. Implementing processes and supplying resources that ensure total compliance comes at a huge cost and would consume a significant amount of a health plan’s resources. An effective and efficient way to address this challenge is to develop a process within the privacy compliance program that assesses risk tolerance, as data privacy issues are part of the majority of transactions and decisions made within a health plan’s day-to-day business.
In response to the above challenges, health plans are working to build best practices within privacy compliance programs. Plans are recognizing the value in making the best use of data and promoting privacy as a core value. Those health plans that focus on this have been most successful because of the effort to integrate privacy compliance into everyday business decisions. Another critical factor in being successful is whether or not the effort is supported by the organization’s leaders. A supportive tone at the top means there is recognition that safeguarding data is good business practice, not just another compliance initiative.