COSMOS
Navigate the Compliance Universe

Health Care Privacy Compliance Handbook, 3rd Edition
5. Payer Privacy Issues

By Debbie R. Mabari [1]

Introduction

What is privacy? Or perhaps more importantly, does privacy still exist in today's interconnected world? Many people view the Fourth Amendment to the Constitution of the United States as implicitly granting a right to privacy:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath...[2]

Most people, therefore, believe that their right to privacy is a given, underscored by law.

However, as computerized data storage and analysis by both private and public organizations become ever more widespread, we have seen a significant erosion in individual privacy.

Thankfully, privacy protections are alive and well when it comes to personal healthcare data. This chapter will explore the impact of privacy regulations in the data-driven payer sector—organizations that provide health insurance and other managed care services.

As discussed in earlier chapters, the U.S. government recognizes the need to safeguard health information separate and apart from other personal information, particularly through the Health Insurance Portability and Accountability Act (HIPAA), which created a set of national standards and practices to safeguard *protected health information* (PHI). Those who must comply with these rules and standards are *covered entities.* Organizations in the payer sector fall primarily in the covered-entity category of *health plan.*[3]

Under HIPAA and related rules, covered entities must protect an individual's PHI collected or created as a result of healthcare operations. See Chapter 1, "HIPAA Privacy and Security," for a deep dive into the wide range of HIPAA requirements. This chapter focuses on key privacy principles that arise with health plans.

Key Principles

Privacy vs. Security

While privacy compliance is much broader than what is in the HIPAA regulations, it is particularly important for payer organizations to be able to distinguish between HIPAA privacy and HIPAA security issues and ensure each are independently addressed.

HIPAA privacy focuses on the right of consumers to control the use of their information. It is also responsive to the expectation of consumers that sensitive information a health plan or provider has about their personal life is only available to the appropriate persons. PHI cannot be used or divulged by others against the consumer's wishes, except where allowed by regulation. The Privacy Rule covers PHI in all formats, including electronic,

paper, and oral, and aims to protect confidentiality—an assurance that information will be safeguarded from unauthorized disclosure.

HIPAA security refers to the methods used to protect the confidentiality of all sensitive information that is transmitted and stored at a health plan or in the custody of those who contract with the health plan, including providers and downstream entities. The Security Rule details how covered entities are expected to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI). The Security Rule also focuses on administrative, technical, and physical safeguards and protection of ePHI from unauthorized access, whether external or internal, stored or in transit.

Portability and Interoperability: *All in One Place*

Before we further explore the privacy mandates that payers have, we should consider a contrasting concept—health data portability. Portability is a term that describes the process or accessing relevant member or patient data remotely, and then utilizing that data locally to support and inform care, as well as improve the member and patient experience. Portability of PHI is a critical component to improving consumer experience by linking the data between insurance companies, hospitals, and physicians, as well as pharmacies and ancillary providers. It allows patients and providers to have access to up-to-date and informed healthcare information across the entire spectrum.

The focus on true portability received a boost in the spring of 2018 from Centers for Medicare & Medicaid Services (CMS) Administrator Seema Verma:

> Imagine a world if you're collecting all of your health-care data from the time of birth all the way through your life.... We want to get to a point where patients have all of their health-care information in one place.[4]

Interoperability is the term used to describe how portability of data is managed across disparate systems. Interoperability typically involves one or more application programming interfaces (APIs) or *bridges* between systems that take data from one source and map that data to an unrelated recipient software application. The use of APIs and other sophisticated data exchange tools is critical to creating an experience that behaves as if consumers have *all their healthcare information in one place.*

There are significant privacy concerns and challenges that come to the forefront as soon as general portability and interoperability are mandated. For example, health information is now being collected and shared across a wide range of mobile and consumer devices, many of which do not meet the standards required for HIPAA-related sharing of PHI. When HIPAA was enacted in 1996, the proliferation of smartphones and tablets along with their ubiquitous apps, plus an exponential increase in the amount of stored and shared data, was unanticipated. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009,[5] which provided updates to HIPAA, set additional standards for the collection, storage, and sharing of medical records and health-related information across covered entities, but does not discuss personal or consumer devices.

So, we are at an important crossroads, where the need to protect patient privacy will be continually weighed against the need to make health information accessible across the entire healthcare spectrum. Constantly changing technology and greater information-sharing capabilities may force legislation to keep pace with these privacy challenges.

Collection, Use, and Disclosure

The HIPAA Privacy Rule allows for some uses and disclosure of PHI and ePHI without an authorization from the consumer, namely for treatment, payment ,and healthcare operations (TPO).[6] Each of these areas will be discussed in detail below, but it is important to note that if a use or disclosure is not permitted, then the information can only be used or disclosed with documented permission and in accordance with the direction of the consumer. Consumers can also request that their personal information be shared with a third party who is their designated representative (e.g., a spouse or parent). Another key provision related to collection, use, and disclosure is the *minimum necessary standard*, which establishes that covered entities must not collect, use, or disclose more personal information than what is needed to accomplish a particular task.[7] This concept is also discussed in detail below.

Treatment, Payment, Healthcare Operations

Treatment includes the provision, coordination, or management of healthcare and related services among healthcare providers or by a healthcare provider with a third party, consultation between healthcare providers regarding a patient, or the referral of a patient from one healthcare provider to another. While such disclosures may be minimal for a health plan, some examples of where it may be applicable include coordination of care efforts, consultation between providers, and referrals to another provider.[8]

Payment includes activity undertaken by the health plan to obtain premiums, to fulfill responsibility for the provision of benefits under the health plan, and to obtain or provide reimbursement for the provision of healthcare. Some examples of payment activities applicable to a plan include determining eligibility or coverage under a plan; adjudicating claims, risk adjustments, billing and collection activities; and utilization review activities.[9]

And finally, the Privacy Rule defines *healthcare operations* as activities compatible with and directly related to conducting quality assessments and improvement activities for the health plan as well as case management, resolving grievances, coordination of care activities, and credentialing. Underwriting, insurance rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits are also considered healthcare operations. Conducting or arranging for a medical review, legal services, and auditing functions, such as fraud and abuse detection, are also activities that allow for use and disclosure by the health plan.[10]

Marketing and Health Plans

Understanding the definition of *marketing* under the HIPAA Privacy Rule is important across the industry, but even more so with health plans, as the marketing department of a health plan helps drive its sales which in turn drive revenue. There are important controls that address whether and how PHI may be used and disclosed for marketing.[11] In general, a written authorization is needed to use PHI for marketing. However, there are some exceptions that health plans should be aware of and which may be important to a health plan's mission of ensuring consumers or beneficiaries receive important information that relates to quality-of-care issues.

It is important to first define what constitutes marketing under the rule. The Privacy Rule defines marketing as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.[12] Simply put, a covered entity may not sell PHI to a business associate or any third party for that party's own purposes. Health plans also may not sell lists of consumers or beneficiaries to third parties without first obtaining an authorization from each person on the list. This part of the definition has no exceptions. An example of marketing that fits the above description would be a health plan that sells a list of its members to a third party that sells blood glucose monitors. The third party purchased the information with

the intent to send the plan's members brochures on the benefits of purchasing and using the monitors. This information cannot be sold without an authorization from every member on the list.

Once marketing is defined, the next step is to identify and understand what marketing is not. The Privacy Rule establishes exceptions to the marketing rules in the following areas:[13]

1. **Refill Reminders**: It is not considered marketing if the communication is made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the consumer; however, if any financial remuneration is received from a third party for making the communication, it must be reasonably related to the health plan's cost of making the communication. For example, a covered entity cannot profit from making the particular communication.

2. **Health-Related Products or Services**: It is not considered marketing if a health plan communication describes a health-related product or service (or payment for such product or service) that is already provided by, or included in the consumer's existing plan of benefits of, the covered entity making the communication. This includes communications about:

    a. The entities participating in a healthcare provider network or health plan network;

    b. The replacement of, or enhancements to, a health plan; and

    c. Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. For example, a health plan may inform members about its own products and services in situations such as communications describing a disease management program that is available to the consumer at no cost.

3. **Treatment, Case Management, or Care Coordination Purposes**: It is not considered marketing if a healthcare provider contacts a consumer as part of the consumer's treatment plan. This area is less applicable to health plans and has more impact on pharmacies or healthcare providers. For example, a provider may contact his/her patient to suggest alternative treatment options, therapies, or other providers.

These additional factors should be considered when reviewing exceptions to the marketing requirements:

- The activity must otherwise be permissible under the Privacy Rule.
- A health plan cannot receive financial remuneration directly or indirectly from a third party whose products or services are being described.
- When using vendors or delegates, a health plan should ensure that a business associate agreement is in place and that the vendor uses the PHI only for communication activities intended by the health plan.

An excellent resource for understanding the practical application of the Privacy Rule, whether about marketing, the minimum necessary standard, or any other provision, is the Frequently Asked Questions section of the U.S. Department of Health & Human Services (HHS) website.[14]