Section 8.0 - Disease Management

James M. Jacobson

8.1 Introduction

Disease management (DM) may be one of the most confusing areas in the Privacy Rule. A key problem is that HHS could not arrive at a definition for DM organizations.[1]

This confusion, in part, exists due to concerns expressed by HHS officials over the use of protected information for marketing purposes. Because many companies that offer DM services also may be engaged in marketing, the department took a function-by-function approach to ensure that protected health information was appropriately handled in any given situation. For a broader discussion of marketing, see Section 7.

As a result, regardless of whether a division or company calls itself a DM organization, the covered entity must examine the specific activities and the target of those activities to determine how the Privacy Rule may apply.

8.2 What is Disease Management?

The Privacy Rule provisions relating to DM are based on two general categories of activity: patient-specific and population-based activities. Many DM programs identify patients in a covered population, such as members of a managed care organization, who have a specific chronic disease (such as diabetes or asthma) that requires substantial management. Under these programs, patient management may include regular patient condition monitoring, medication compliance advice and recommendations to the physician for adjustments and self-management training.

The DM organization also may operate a system in which it advises health professionals on "best practices" or evidence-based treatment guidelines developed from outcomes research. They also may include telephone and web-based interactions with patients to monitor their progress and allow them to seek further information.

As discussed in Section 5.0, covered entities generally are required to obtain patient authorizations for uses and disclosures of protected health information other than for treatment, payment or health care operations.

The challenge for covered entities is determining when DM activities qualify as treatment or health care operations, which will not require patient authorization, as opposed to marketing or some other non-treatment, non-health care operations activity, which will require patient authorization for the use and disclosure of protected health information.

8.3 Application to the Privacy Rule

Covered entities may use or disclose protected health information to DM organizations without patient authorization for treatment and health care operations. Treatment in this context generally refers to activities directed toward a specific patient. Health care operations in this context generally refers to activities that are aimed at populations of patients.

8.3.1 Patient-Specific Activities

Covered entities may use or disclose protected health information to their DM organizations without patient authorization under the treatment exception if the DM services are directed toward a particular individual and if a provider is involved in the use or disclosure.

The Privacy Rule defines treatment to mean:

> ... the provision, coordination, or management of health care and related services by one

> or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.[2]

DM activities involving a nurse or other clinician aimed at specific individuals generally would fall under the Privacy Rule's definition of treatment and thus would not require patient authorization. Some common activities in this area include:

- Nurse chat;
- Patient self-management coaching;
- Medication usage and compliance information (which also may fall within the definition of health care operations);
- Interactions with patients via telephonic or Web-based DM tools; and
- Other activities that engage the patient in individualized health care improvement.

It is still unclear whether health plans (both staff model plans, which really are providers, and group model or other non-staff plans which are not) may take advantage of the treatment exception. Recent guidance has shed no light on this aspect of the rule. The treatment definition says nothing about health plans, and the preamble states that "Activities of health plans are not considered to be treatment."[3]

Until further guidance is provided, health plans cannot be assured that that they may use and disclose protected health information for those DM activities focused on specific individuals under the treatment exception. However, health plans may still use and disclose protected health information for most DM purposes under the health care operations exception to the patient authorization requirements.

8.3.2 Population-Based Activities

Covered entities also may use or disclose protected health information to their DM vendors without patient authorizations if the activity falls under health care operations. In other words, the Privacy Rule authorizes covered entities such as HMOs, insurers, and employer ERISA health plans to use and disclose protected health information for DM activities that are population-based without patient consent or authorization.

Some common activities in this area, as described in the definition of health care operations, include:

- Quality assessment and improvement, including outcomes evaluation and development of clinical guidelines;
- Population-based activities related to improving health or reducing health care costs;
- Protocol development;
- Case management and care coordination;
- Contacting health care providers and patients with information about treatment alternatives; and
- Related functions that do not include treatment.

8.4 Compliance Considerations

Until HHS offers guidance or modifications to the final rule, covered entities should take the following steps to achieve compliance with the patient authorization and consent provisions of the rule:

8.4.1 Covered Entities

A. Patient Authorizations and Consents: All covered entities should:

- Determine which exceptions to patient authorization and consent might apply to internal and outsourced DM programs.
- If patient authorization or consent is required or desired for any DM uses or disclosures, ensure that the patient forms specifically permit access to protected health information for DM purposes, and otherwise conform to regulatory requirements for consent forms.
- Review and conform compliance to state laws that are more stringent.

B. Health Care Providers: Health care providers, when acting as covered entities, should:

- Obtain patient consent when using or disclosing protected health information for DM purposes, regardless of whether the DM activities are focused on a particular patient (treatment) or a population (health care operations).
- To avoid the need for obtaining a patient authorization when using or disclosing protected health information for DM activities focused on a specific patient, ensure that

providers develop the protected health information themselves or receive it directly from a patient.

If providers receive the protected health information at any point from a health plan or other non-provider covered entity, it is not clear whether such providers, as Business Associates to the health plan covered entity, could use it for a "treatment" purpose without patient authorization, because the health plan arguably could not do so.

C. Health Plans: Health plans, when acting as covered entities, should:

- Determine whether specific uses or disclosures of protected health information for DM activities come within the treatment or health care operations exceptions. If they are not specifically enumerated items in the health care operations definition, opinion of counsel should be sought regarding whether patient authorizations are required.
- For patient and employer relations and for risk management purposes, determine whether to seek patient consents for those DM activities within treatment and health care operations even though not required by the Privacy Rule. HHS recognized in the Preamble that health plans, including ERISA welfare benefit plans, may have a higher comfort level that they will not be sued under state tort or contract law for violating HIPAA provisions (e.g., when a state has set HIPAA compliance as the state standard of privacy compliance) when they have a tangible patient consent on file especially when authorizations are not required.

8.4.2 "Minimum Necessary" Disclosure and DM

A covered entity must ensure that no more than the "minimum necessary" protected health information is used or disclosed, and must implement appropriate policies and procedures to carry out this purpose. Comments on the Privacy Rules specifically state that the "minimum necessary" standard is intended to reflect and be consistent with, not override, professional judgment and standards.

However, there will be a substantially greater liability risk for covered entities that are used to disclosing entire medical records to their DM vendors or pharmacy benefit managers if they do not carefully analyze whether continuing that practice would comply with the rule's intent. HHS's first round of clarifications significantly relaxes may of these concerns by establishing a "reasonable" business practices standard.[4]

For DM purposes, the Privacy Rule distinguishes between the use, request, and disclosure of protected health information:

- Use: A covered entity must identify and document whether its DM programs, internal or outsourced, have a need for protected health information and the categories of protected health information to which such programs need access.
- Disclosure: A covered entity must implement policies and procedures that limit the routine and recurring disclosure of DM information to the minimum that is necessary for the particular DM purpose. The covered entity is not required to review each routine and recurring disclosure individually.
- Request: For all other disclosures, a covered entity must develop criteria that limit disclosure to that necessary to comply with a specific request by a DM vendor. The covered entity must individually review every request for disclosure according to the developed criteria. Disclosures to health care providers for treatment purposes are not subject to these requirements.

8.4.3 DM and Business Associate Agreements

Generally, a covered entity may disclose protected health information to a Business Associate, or hire a Business Associate to obtain or create protected health information for it, but only if the covered entity obtains specified satisfactory assurances through a written agreement that the Business Associate will appropriately handle the information. (See Section 6.0 for a fuller discussion of Business Associate agreements).

Covered entities offering DM programs through outsourced DM organizations, PBMs, and others generally will have to have Business Associate contracts with them.

Covered entities should:

- Ensure that the Business Associate agreement includes a statement of the specific DM activities to be delegated, with vendor assurances that it will safeguard such protected health information as required by contract and by the use and disclosure rules applicable to the covered entity;
- Determine whether to limit disclosures of protected health information to DM Business Associates only for the purposes of carrying out those DM activities that are listed within the treatment or health care operations exceptions to patient authorization. With such limitations, the covered entity may avoid potential liability for the DM organization's failures to obtain authorizations on its behalf.
- If the covered entity does not wish to limit protected health information disclosures to its DM organization to those within the exceptions to patient authorization, the Business Associate contract should:

    1. Ensure that the DM organization will obtain a patient authorization as required by the rule for all uses or redisclosures for DM purposes that are not treatment and health care operations; or
    2. Require consultation between the covered entity and the DM organization's legal staff to make a determination as to whether patient authorizations are required; or
    3. Require an opinion of outside counsel or, if possible, advice from HHS itself.

- Ensure that the contract requires DM vendors to include all of the same provisions of the Business Associate agreement in any subcontracts it enters into on behalf of the covered entity. For example, DM vendors may themselves outsource to web-enabling firms to add Internet care management tools, home monitoring device companies, and nurse triage/demand management firms.
- Strict scrutiny of the vendor's subcontracting agreements should be mandated in the Business Associate agreement. The covered entity may wish to go even further by requiring the DM vendor to get its approval before redisclosing protected health information to subvendors (other than to providers), or by requiring the use of covered entity-prepared Business Associate contracts for use with subvendors.
- Require DM vendors to report any known misuse of protected health information by itself or a subvendor to the covered entity.
- Require termination of the contract if the covered entity has substantial and credible evidence of a pattern or practice of the DM vendor that is a material breach of the agreement related to the use or disclosure of protected health information and the minimum necessary rule.
- Require the DM vendor, upon termination, to return or destroy all protected health information provided to it by the covered entity.
- Require the DM vendor to name the covered entity as an insured on its errors and omissions policies, and ensure that the policies cover HIPAA and state privacy law breaches.
- Require the DM vendor to comply with all state laws that are not preempted.
- Require careful indemnification provisions that specifically indemnify the covered entity from liabilities incurred due to DM vendor uses and disclosures of protected health information.

8.4.4 DM and Administrative Obligations

Other sections have already described the administrative and consumer protection requirements. While only a few of these provisions have specific implications for DM programs, they are significant. First, because there is so much confusion about whether a covered entity may use or disclose to the vendor protected health information for DM services that are not specifically enumerated in treatment or health care operations, the following are among those most critical for covered entities to consider:

- Covered entities must train their workforce appropriately concerning which protected health information, and for which purposes protected health information, may be disclosed. For example, marketing staff or other business people usually will not have enough

clinical information to know whether certain databases of claims, laboratory, and prescribing data or medical records will be used by the DM vendor for enumerated treatment or health care operations purposes.

- Because privacy practices are likely to change frequently with respect to DM programs as the industry itself matures, covered entities should include in the patient notice of information practices a provision that expressly reserves the right to change its privacy practices. Otherwise, the covered entity will be required to follow the burdensome procedures outlined in the Privacy Rule to make changes.

8.5 Key Points

The following key points were made in this section:

- Because HHS did not define DM, covered entities must take a function-by-function approach in determining how to comply with the Privacy Rule.
- DM activities generally fall into two categories: patient specific and population based. Patient-specific activities are likely to be deemed treatment while population-based activities are likely to be deemed health care operations.
- Covered entities generally will require Business Associate contracts with their DM vendors.
- Covered entities should be sure to include in their notices on privacy practices that they reserve the right to change those policies as DM services are likely to change as they mature.

Endnotes

[1] HHS stated in the preamble: "Many commenters recommended adding the term disease management to health care operations. We were unable, however, to find a generally accepted definition of the term. Rather than rely on this label, we include many of the functions often included in discussions of disease management in this definition or in the definition of treatment." 65 Fed. Reg. at 82,490.

[2] *id.* at 82,805 (to be codified at 45 C.F.R. pt. 164.501).

[3] 65 Fed. Reg. at 82,498.

[4] *Guidance/Q&As*, Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. pts. 160 and 164), *available at* http://www.hhs.gov/ocr/hipaa (last revised July 6, 2001)