GLASER & WEINER, LLP

HEALTH LAW UPDATE

October 2009

In recent months, several significant laws have been passed requiring the attention of home health agencies – compliance plans, red flags rules, breach notification laws, new business associate requirements, not to mention flu vaccination mandates and registry implementation. Providers have been challenged to sort out the new requirements and figure out what to do next. The Long Island Chapter/HCP has asked us to prepare the following summary of three recent initiatives: the New York State mandatory compliance program requirement for Medicaid providers, the Red Flags Rules and the HITECH breach notification and business associate requirements, and to provide recommendations for action.

OMIG COMPLIANCE PLANS

What: The New York State Office of the Medicaid Inspector General (OMIG) adopted new regulations requiring implementation of mandatory compliance programs by all Article 36 (home health care) Medicaid providers.

When: The effective date of these regulations is July 1, 2009 and all covered providers must be in compliance as of September 29, 2009. Providers participating in Medicaid will need to certify every December that they meet the requirements of these regulations.

What are Providers Required to Do: To be effective, a compliance program must reflect a provider's size, complexity, resources and culture. It must also be designed to be compatible with a given provider's characteristics. However, the new law contains a set of minimum core requirements that are applicable to all providers, regardless of size, that are subject to its provisions.

The basic statutory requirements for elements that must be included in a compliance program are as follows:

- **Written policies and procedures** that describe compliance expectations, as embodied in a code of conduct or code of ethics; implement the operation of the compliance program; provide guidance to employees and others on dealing with potential compliance issues; identify how to communicate compliance issues to appropriate compliance personnel; and describe how potential compliance problems are investigated and resolved.

- **Designate an employee vested with responsibility for the day-to-day operation of the compliance program**; this employee's duties may solely relate to compliance or may be combined with other duties so long as compliance responsibilities are satisfactorily carried out; this employee will report directly to the entity's chief executive or other

senior administrator and will periodically report directly to the governing body on the activities of the compliance program.

- **Training and education** of all affected employees and persons associated with the provider, including executives and governing body members, on compliance issues, expectations and the compliance program operation; this training must occur periodically and must be made a part of the orientation for a new employee, appointee or associate, executive and governing body member.

- **Communication lines** to the responsible compliance position, as described in the second bullet above, that are accessible to all employees, persons associated with the provider, executives and governing body members, **to allow compliance issues to be reported**; the communication lines shall include a method for **anonymous and confidential good faith reporting** of potential compliance issues as they are identified.

- **Disciplinary policies** to encourage good faith participation in the compliance program by all affected individuals, including policies that articulate expectations for reporting compliance issues and assist in their resolution and outline sanctions for: (1) failing to report suspected problems; (2) participating in non-compliant behavior; or (3) encouraging, directing, facilitating or permitting non-compliant behavior.

- A **system for routine identification of compliance risk areas** specific to the provider type, for self-evaluation of these risk areas, including internal audits and as appropriate external audits, and for evaluation of potential or actual non-compliance as a result of self-evaluations and audits.

- A **system for responding to compliance issues** as they are raised; for investigating potential compliance problems; responding to compliance problems as identified in the course of self-evaluations and audits; correcting problems promptly and thoroughly and implementing procedures, policies and systems as necessary to reduce the potential for recurrence; identifying and reporting compliance issues to the OMIG or the DOH; and refunding overpayments.

- A **policy of non-intimidation and non-retaliation** for good faith participation in the compliance program, including but not limited to reporting potential issues, investigating issues, self-evaluations, audits and remedial actions, and reporting to appropriate officials as provided in sections seven hundred forty and seven hundred forty-one of the labor law (new whistleblower provisions for health care fraud).

Failure by a provider to implement a satisfactory compliance program within ninety days after the effective date of the regulations will subject the provider to sanctions or penalties including, but not limited to, the revocation of the provider's agreement to participate in the Medicaid program.

RED FLAGS RULE

What: The Red Flags Rule is an anti-fraud regulation issued by the Federal Trade Commission (FTC), requiring "creditors" and "financial institutions" with covered accounts to implement programs to identify, detect, and respond to the warning signs, or "red flags," that could indicate identity theft. The FTC has confirmed that healthcare providers that regularly offer credit or payment plans to patients, or that allow patients to pay over time in installments, must comply with the rule. The rule does not apply to entities that accept payment by credit card only on a single-transaction basis.

When: Compliance is required by November 1, 2009.

What are Providers Required to Do: Affected organizations must create and institute a **written program** appropriate to their size and operations that:

- **Identifies "red flags"**--patterns, practices, and specific forms of activity that indicate the possible existence of identity theft--and provides procedures for detecting them in day-to-day operations;
- **Proposes responses if red flags are detected** in order to prevent identity theft for occurring or to reduce its effect if it has already occurred;
- **Provides for training** of staff and **oversight** of any service providers;
- Provides a **plan for periodic updating of the program**; and
- Is **well-documented and approved** by the board of directors, board committee, or senior management (if there is no board).

Some red flags that might arise in a health care context include:

- A complaint or question from a patient based on the patient's receipt of:
    - a bill for another individual;
    - a bill for a product or service that the patient denies receiving;
    - a bill from a health care provider that the patient never patronized; or
    - a notice of insurance benefits for health services never received.
- Records showing provision of care that is inconsistent with the physical examination or a medical history as reported by the patient;
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft; or
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

HITECH ACT

The HITECH Act has two components requiring action: requirements for notification of breaches of unsecured PHI and extension of certain HIPAA Security and Privacy rules directly to business associates.

Notification of Breaches of Unsecured PHI

What: The Department of Health and Human Services (HHS) published rules that lay out the specific steps that HIPAA-covered entities and their business associates must take in the event of a breach of unsecured protected health information (PHI).

When: The rules related to breaches of unsecured PHI became effective September 23, 2009. HHS has stated that while it expects covered entities to comply with this Rule as of September 23, 2009, it will not impose sanctions for failure to provide the required notifications for breaches discovered through February 22, 2010. Instead, during this period HHS will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

What are Providers Required to Do: The HITECH Act requires covered entities to notify individuals whose PHI has been disclosed because of a breach of security, but only if that PHI was "unsecured". Business associates are also required to notify covered entities of such breaches. The term "unsecured" means that the PHI is not secured through the use of certain technologies or methodologies (encryption or destruction) that render the information unusable and indecipherable to unauthorized persons. If covered entities and business associates maintain PHI using the required technologies and methodologies, they do not hold "unsecured PHI" and would not have to report breaches if any occur.

Providers should develop an action plan for how they will respond in the event of a breach of unsecured PHI.

Business Associates

What: The HITECH rules also make certain HIPAA privacy and security rules directly applicable to business associates "in the same manner that such sections apply to the covered entity." This may require amendment to your business associate agreements, however, there is no consensus yet among the health law community as to what revisions to business associate agreements should look like. We are awaiting HHS regulations clarifying this.

When: The HITECH rules pertaining to business associates become effective on February 17, 2010.

What are Providers Required to Do: Regulations that outline the HITECH Act's effects on business associate agreements are due to be published before the regulations

take effect. In the interim, if providers' business associate agreements do not already contain a provision that automatically updates and incorporates changes in laws and regulations into the agreement, a sample provision that may be inserted into existing or new business associate agreements is found below. This should be discussed with your legal counsel before implementing.

Sample interim business associate agreement language: The parties agree to take such action to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule, the Security Rule, and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191. In addition, the parties agree that, prior to February 17, 2010 (or such extended time as permitted by statute), they shall amend this Agreement to incorporate the provisions required pursuant to Title XII of the American Recover & Reinvestment Act of 2009 (ARRA), also known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. Specifically, this Agreement shall be revised to provide that (a) provisions of the HIPAA Security Rule shall directly apply to the Business Associate in the same manner as it applies to the Covered Entity and (b) the Business Associate shall be bound by additional Privacy Rule-related obligations.

Providers should adopt policies outlining how they will relate to their business associates in light of these new rules.