DEVINE MILLIMET

ATTORNEYS AT LAW

HIPAA AND HITECH

January 26, 2010

Presented by:
Sandra K. Mann, Esquire
Devine, Millimet & Branch, P.A.
111 Amherst Street
Manchester, NH 03101
603.695.8656
smann@devinemillimet.com

DEVINE MILLIMET

ATTORNEYS AT LAW

Questions on my presentation in the morning.

DEVINE MILLIMET
ATTORNEYS AT LAW

Accounting for Disclosures

- Covered entities are required to account to the individual for certain disclosures of PHI in the six years prior to the date on which the patient makes the request. (45 CFR § 164.528)
- Exceptions to this rule (not inclusive):
  - Treatment, payment and health care operations;
  - Incident to a use or disclosure;
  - Pursuant to a valid authorization;
  - Facility directory;
  - Persons involved in the individual's care;
  - As part of a limited data set.
- Accountings are required for disclosures for governmental oversight activities, i.e., disclosures to DHHS.
- System will account to disclosures/uses by DHHS.

DEVINE MILLIMET
ATTORNEYS AT LAW

Revisions of HIPAA Notice of Privacy Practices

- Participation in the Employment Indicator System should not conflict with any HIPAA policies and procedures.
- Nonetheless, review your Notice of Privacy Practices to ensure that it is up-to-date, consistent with your internal policies and procedures, and does not conflict with participation in the Employment Indicator System.

DEVINE MILLIMET

ATTORNEYS AT LAW

Health Information Technology for Economic and Clinical Health Act (HITECH)

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

1) Business Associate Agreements (Effective February 18, 2010).

   HITECH applies many of the HIPAA rules directly to business associates. Under HITECH, business associates must comply with the:

   - Administrative, physical, and technical safeguard requirements of the HIPAA Security Rule, as well as the requirement to maintain policies, procedures, and documentation of security activities in the same manner that applies to covered entities;
   - The new breach reporting requirements under HITECH;
   - The applicable requirements under 45 CFR § 164.504(e);

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

1) Business Associate Agreements (Continued).

- Business associates will also take reasonable steps to cure a pattern of activity by or a practice of the covered entity that constitutes a material breach or violation of the covered entity's obligation under the business associate agreement, unless the covered entity took steps to cure such breach or violation. If such steps are unsuccessful, the business associate must terminate the agreement, and if that is not feasible, then report such breach or violation to the U.S. DHHS.

  (HITECH §§ 13402 and 13404).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

2) Restrictions on Disclosures to Health Plans.

- HIPAA currently permits an individual to request a restriction on the covered entity's use and disclosure of PHI, but the covered entity is not required to agree to the restriction. (45 CFR § 164.522(a)(1)(i)-(ii)).
- HITECH prohibits a covered entity from refusing an individual's request not to use or disclose the individual's PHI where the disclosure is to a health plan for purposes of carrying out payment, treatment, and the PHI pertains to a health care service for which the provider involved has been paid out-of-pocket in full.
- An identical requirement exists under State regulations. See He-M 309.05(e)(4), He-M 310.05(e)(4).

(HITECH § 13405(a)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

3) Changes to the Minimum Necessary Standard.

- HITECH requires covered entities, when using or disclosing PHI, or requesting PHI, to limit "to the extent practicable" disclosure of PHI to the "limited data set" as defined under HIPAA, or if more information is necessary, to the minimum necessary "to accomplish the intended purpose of such use, disclosure, or request."
- HIPAA currently permits covered entities to rely on a request by other covered entities as being the "minimum necessary" for a particular disclosure. HITECH requires the covered entity to make the determination of minimum necessary for disclosure.

(HITECH § 13405).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

3) Changes to the Minimum Necessary Standard (Continued).

- These minimum necessary requirements sunset when the U.S. DHHS issues guidance on what constitutes "minimum necessary" for purposes of PHI disclosure.
- All current exceptions to the minimum necessary rules remain in place, e.g., treatment, required by law.

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

4) Expansions of Accounting for Disclosures.

- HIPAA requires covered entities to provide an "accounting" of disclosures of PHI to individuals at their request.
- There are various exceptions to this rule, including disclosures made for payment, treatment and operations.
- HITECH removes the accounting exception for disclosures of PHI to carry out treatment, payment, and health care operations. All such disclosures must be accounted for if made through an electronic health record.

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

4) Expansions of Accounting for Disclosures (Continued).

- Only applies to 3 years, not 6 years.
- HITECH permits covered entities to either provide the requesting individual with an accounting of disclosures of PHI made by the covered entities business associate, or provide a list and the necessary contact information for all relevant business associates.

(HITECH § 13405(c)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

5) Prohibition on Sale of PHI.

- Under HITECH, covered entities may not receive remuneration, indirectly or directly, in exchange for an individual's PHI without obtaining that individual's authorization.
- Exceptions (subject to other laws):
  - Public health activities;
  - Research;
  - Treatment;
  - Sale, transfer, merger or consolidation of all or part of the covered entity and due diligence related to such activity;
  - For an activity undertaken by a business associate on behalf of a covered entity, where remuneration is provided by the covered entity;
  - Providing an individual with a copy of his or her PHI in a designated record set.

(HITECH § 13405(d)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

6) Mandated Access to Electronic Copies of PHI Contained in an EHR.

- A covered entity that uses or maintains an EHR (as defined in HITECH) with respect to PHI is required to produce a copy of such PHI in an electronic format upon an individual's request, and upon the individual's request, transmit such information to a third party.
- The covered entity may impose a fee which may not be greater than the labor costs involved in responding to the request.

(HITECH § 13405(e)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

7) New Restrictions on Marketing (Effective Date: February 17, 2010).

Under HITECH, covered entities cannot receive remuneration, indirect or direct, in exchange for making permissible communications under the current HIPAA rules, unless:

- Such payment is for a communication regarding a drug currently prescribed for the recipient of the communication, and such payment is "reasonable in amount";
- The communication is made by the covered entity, and the covered entity obtains a valid authorization from the individual; or
- The communication is made by a business associate of the covered entity, on behalf of such covered entity, and such communication is consistent with the applicable business associate agreement.

(HITECH § 13406(a)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

8) Opt Out of Fundraising.

- HIPAA requires that any written fundraising communication that is a health care operation shall be communicated in a clear and conspicuous manner and provide an opportunity for the recipient of the communications to elect not to receive any further communications. (45 CFR § 164.514(f)(2)).
- Under HITECH, the rule does not change but the "opt out" is treated as a revocation of the authorization.

(HITECH § 13406(b)).

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

8) Opt Out of Fundraising (Continued).

- Use and Disclosure of Protected Health Information Marketing; Fundraising. RSA 332-I:4, Effective January 1, 2010.
  - Health care providers and business associates of health care providers shall obtain authorization for any use or disclosure for PHI for marketing.
  - With respect to fundraising, the new State law mirrors HITECH, but requires:
    - Simple election language and font of sufficient size to be easily readable by the average adult reader.
    - Opportunity to opt-out must be 60 days prior to the communication or placed in the notice of privacy practices so long as the individual receives the NPP prior to the fundraising communication.

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

9) Security Breaches.

- Extensive new requirements for reporting and monitoring security breaches. Covered entities and business associates are required to notify individuals of a breach of unsecured protected health information.
- Unsecured protected health information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in guidance issued by DHHS and posted on its website.
- Notification must be to each individual whose PHI has been or is reasonably believed by the covered entity to have been disclosed, accessed, acquired, used or disclosed as a result of the breach.

DEVINE MILLIMET
ATTORNEYS AT LAW

New Requirements Under HITECH

9) Security Breaches (Continued).

- Regulations dictate the content and timeliness of the notification to the affected individual.
- Notification to the media is required for breaches involving more than 500 residents of a state or jurisdiction.
- Notification to the Secretary of the U.S. DHHS is required for breaches involving (i) 500 or more individuals contemporaneously with the notification sent to such individuals; (ii) less than 500 individuals, annually.
- Business associates shall notify the covered entity of the breach, and shall provide the notification.

(HITECH § 13401; 74 Fed. Reg. 42740 (August 24, 2009).

DEVINE MILLIMET
ATTORNEYS AT LAW

Implications of HITECH

- Revise business associate agreements.
- Develop a security breach policy for compliance with HITECH and State law (RSA 359-C:19).
- Review notice of privacy practices for compliance with the fundraising and marketing rules.
- Monitor DHHS activities for the publication of additional guidance and proposed regulations.

DEVINE MILLIMET

ATTORNEYS AT LAW

Questions