WHAT EVERY MUNICIPALITY SHOULD KNOW ABOUT HIPAA'S MEDICAL PRIVACY RULES

Presentation to the

International Municipal Lawyers Association
2003 Mid-Year Seminar

Andrea I. O'Brien
Venable LLP©
April 28, 2003

TABLE OF CONTENTS

Page

Introduction 1

FOUR GENERAL THINGS MUNICIPALITIES SHOULD KNOW ABOUT HIPAA'S ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS AND PRIVACY RULE 3

WHAT DOES THE HIPAA PRIVACY RULE MEAN FOR MUNICIPALITIES 5

Compliance Issues for Municipalities that Sponsor Self-Insured Group Health Plans that Cover at Least 50 Participants or Use a TPA 5

Compliance Issues for Municipalities that Sponsor Fully-Insured Group Health Plans 11

Compliance Issues for Municipalities that Provide On-Site Health Care 12

A MUNICIPALITY'S PRELIMINARY CHECKLIST FOR COMPLIANCE WITH HIPAA'S ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS AND PRIVACY RULE 15

Step #1 – Identification 15

Step #2 – Analysis 15

Step #3 – Authorization 18

Step #4 – Review on-site medical services and other programs 18

FAQS: FREQUENTLY-ASKED QUESTIONS ABOUT A MUNICIPALITY'S OBLIGATIONS UNDER HIPAA'S PRIVACY RULE 19

Scope of the HIPAA Privacy Rule 19

Uses of PHI Under the HIPAA Privacy Rule 20

Administrative Procedures and Requirements 21

Impact of HIPAA Privacy Rule on Employment Practices 21

Compliance Steps for Municipalities 22

Liability, Penalties and Enforcement 23

WHAT EVERY MUNICIPALITY SHOULD KNOW ABOUT HIPAA'S MEDICAL PRIVACY RULES

INTRODUCTION

HIPAA is shorthand for a Federal law called the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) and a host of rules it has generated concerning the handling of health care information by health plans, certain health care providers, health care clearinghouses (*"covered entities")* and entities that do work for them (*"business associates"*). HIPAA, among other things, establishes administrative simplification requirements, electronic transaction standards, security requirements and privacy rules which set minimum standards on when and how covered entities can exchange *protected health information* (PHI)[1] with other covered entities and third parties.

Compliance with the electronic transactions standards was required by October 16, 2002, although many covered entities obtained a one-year extension until October 16, 2003. 45 CFR § 162.900. Compliance with the privacy rules was required by April 14, 2003 for health care providers and large health plans, and is extended until April 14, 2004 for smaller health plans, defined as plans with less than $5 million in annual receipts. 45 CFR § 164.534. Compliance with the security standards is not required until April 21, 2005 for health care providers and large plans, and April 21, 2006 for smaller health plans. 45 CFR § 164.318.

A municipality is likely to be subject to HIPAA in two different ways:

(1) First, to the extent that a municipality maintains an on-site facility or other program constituting a *health care provider*[2], the municipality must ensure that the facility and/or program complies with these rules if that facility or program conducts certain transactions electronically. 45 CFR § 160.103.

---

[1] PHI is *individually identifiable health information* (i.e., health information that identifies the individual to whom it relates or could be used to identify that individual, which is created or received by a covered entity or a municipality) maintained or transmitted by a covered entity. 45 CFR § 164.501. PHI can range from information about an individual's medical condition to his premium payment information or eligibility under a health plan.

[2] The definition of a health care provider includes any entity which, in the normal course of its business, furnishes, bills or is paid for *health care*. 45 CFR § 160.103. The Privacy Rule defines health care broadly to include, but not be limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body. 45 CFR § 160.103.

(2) In addition, most group health plans sponsored by municipalities are subject to the HIPAA rules, even though the municipalities themselves are not considered "covered entities" subject to HIPAA. 45 CFR § 160.103. The compliance burden is especially significant for municipalities that sponsor a self-insured group health plan that covers 50 or more participants or that uses a *third-party administrator (TPA)*, because the individuals responsible for administering the self-insured medical plan are usually employees of the sponsoring municipality. Unlike HIPAA's portability rules, from which self-funded governmental plans can "opt out", the privacy rules apply uniformly to health plans sponsored by both public sector and private sector employers.

What follows is a summary guide for complying with HIPAA's medical privacy rules. With preamble and regulations exceeding 1000 pages, it is impossible to summarize all of HIPAA's complex requirements here. This summary is intended to provide general information and education about HIPAA's administrative simplification requirements and, in particular, its privacy rules and their impact on municipalities. You should not act or rely upon the information provided in this summary without first seeking the advice of an attorney who is familiar with your situation.

FOUR GENERAL THINGS MUNICIPALITIES SHOULD KNOW ABOUT HIPAA'S ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS AND PRIVACY RULE

⇒ Congress, through HIPAA, wants health plans and health care providers to standardize the way they package health information for electronic transmission – the goal being a health information system that is more efficient and effective. These electronic transactions standards are final, and the *deadline for compliance was October 16, 2002.* A one-year extension until *October 16, 2003* was available if appropriately requested on or before October 15, 2002, and was automatically granted to "small" health plans. 45 CFR § 162.900.

HIPAA Goal
Creating standards for electronic transactions

⇒ With the electronic transfer of health information comes concerns about protecting the privacy of the information that is being transmitted. Congress, through HIPAA, wants to make sure that the sharing of standardized health information does not occur at the expense of individual privacy, and that municipalities do not use health information to make employment-related decisions. Therefore, HIPAA sets minimum standards on when and how *covered entities* can exchange *protected health information* (PHI) with other covered entities and with third parties. These rules are final. For health care providers and "large" health plans, compliance is required by *April 14, 2003*; for "small" health plans, compliance is required by *April 14, 2004*. 45 CFR § 164.534.

HIPAA Goal
Ensuring the safe exchange of health information

⇒ Congress, through HIPAA, wants to make sure that *covered entities* protect health information carefully by maintaining appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of information. Security standards require covered entities to provide these safeguards and were recently finalized, to take effect on *April 21, 2005* (or *April 21, 2006* for "small" health plans). 45 CFR § 164.318.

HIPAA Goal

Security measures to safeguard health information

⇒ If you are a *covered entity* and you fail to comply with HIPAA's rules, you may face a penalty of $100 for each violation (with total exposure of no more than $25,000 for all violations of an identical requirement). 42 USC § 1320d-5. If you knowingly violate HIPAA in your use or disclosure of PHI, fines can range from $50,000 to $250,000 and/or imprisonment of up to one year, five years or ten years, depending on the circumstances of the use or disclosure. 42 USC § 1320d-6.

WHAT DOES THE HIPAA PRIVACY RULE MEAN FOR MUNICIPALITIES?

Compliance Issues For Municipalities That Sponsor Self-Insured Group Health Plans That Cover At Least 50 Participants Or Use A TPA

In order to ensure that its self-insured group health plans comply with HIPAA's administrative simplification requirements and Privacy Rule, a municipality must focus on four key areas:

- Administrative policies and procedures
- Notification to participants
- Plan documentation and certification
- Contracts with business associates

Each of these areas is described below.

⇒ ***Administrative Policies and Procedures***

Municipalities sponsoring self-insured group health plans must, on behalf of their plans, establish and implement new administrative policies that will guard against the improper use or disclosure of PHI, as well as address any grievances or complaints from plan participants about the improper use or disclosure of PHI. 45 CFR § 164.530. These policies and procedures include the following:

√ *Establish an Overall HIPAA Privacy Policy*

The municipality sponsoring a self-insured group health plan should develop and distribute a written policy for the plan that includes the following:

♦ A statement that the plan will comply with HIPAA's administrative requirements and Privacy Rule, and referring participants to consult the new administrative procedures that have been established to address concerns or complaints. 45 CFR § 164.530(i); 45 CFR § 164.530(d).

♦ A statement that sanctions and disciplinary action will be imposed against any member of the municipality's workforce who fails to comply with the rules, or who intimidates or retaliates against individuals who exercise their rights under the Privacy Rule. 45 CFR § 164.530(e); 45 CFR § 164.530(g).

- A reservation of the right to change or modify the policy at any time in the future, in its sole discretion, or in compliance with the law.

√ *Designate a Privacy Official and Contact Person, and Establish Administrative Procedures for Complaints*

- The sponsoring municipality, on behalf of the plan, must appoint and designate an individual to serve as the *"Privacy Official"*, who will be responsible for the development and implementation of the plan's privacy policies and procedures, and a "*Contact Person*", who will be responsible for receiving complaints and providing information. 45 CFR § 164.503(a)(1). Although these individuals will normally be employees of the municipality, they will serve in these roles on behalf of the plan.

- The sponsoring municipality, on behalf of the plan, should then develop internal, administrative procedures that will provide a process for individuals to make complaints concerning the plan's privacy policies or its compliance with them or with the Privacy Rule. 45 CFR § 164.530(d).

- The sponsoring municipality must establish a process for documenting all complaints received, and their disposition, if any. 45 CFR § 164.530(d).

- The sponsoring municipality must mitigate, to the extent practicable, any harmful effect from the improper use or disclosure of PHI. 45 CFR § 164.530(f).

√ *Revise Enrollment Materials*

All enrollment materials for the self-insured group health plan should be reviewed to make sure that the plan does not require individuals to waive their rights under the Privacy Rule as a condition of enrollment or eligibility for benefits. 45 CFR § 164.530(h).

√ *Establish Technical and Physical Safeguards*

The sponsoring municipality, on behalf of the plan, must establish appropriate procedures and safeguards for protecting PHI from being used or disclosed – either accidentally or intentionally – except as permitted under HIPAA. These safeguards should be both technical (*e.g.*, eliminating access to information by creating computer firewalls) and physical (*e.g.*, locking doors or filing cabinets). 45 CFR § 164.530(c).

√ *Develop a Document Retention Policy*

The sponsoring municipality must establish and implement a document retention policy, so that the plan keeps copies of all privacy policies and procedures which are adopted, as well as any other communications, authorizations, or other written documents required by the HIPAA administrative requirements and Privacy Rule to be in writing, for at least 6 years. 45 CFR § 164.30(j).

√ *Identify and Train All Necessary Personnel*

- The sponsoring municipality must train all members of its workforce who may receive PHI, on behalf of the plan, about the plan's privacy policies and procedures. 45 CFR § 164.530(b).

- The sponsoring municipality must develop a process for documenting the training.

- The sponsoring municipality must have and apply appropriate sanctions against members of its workforce who fail to comply with the Privacy Rule or with the plan's privacy policies and procedures. 45 CFR § 164.530(e).

- The sponsoring municipality must develop a process for documenting any sanctions applied.

⇒ ***Notification to Participants***

A municipality that sponsors a self-insured group health plan that covers at least 50 participants or uses a TPA must develop a *Notice of Privacy Practices* for the plan, and periodically distribute that Notice to the plan's participants. This Privacy Notice must describe how the participants' PHI may be used and disclosed, and how the participants can access that information. 45 CFR § 164.520. The Privacy Notice must include among other things, the following information:

√ *A Summary of the Privacy Rules and a Description of PHI*

The Privacy Notice must state that the plan is required by law to maintain the privacy of PHI and to provide individuals with notice. This general statement should describe PHI and include examples of the permitted uses and disclosures of PHI. 45 CFR § 164.520(b)(1)(ii) and (iii).

√ *Participant's Right to Information*

The Privacy Notice must briefly describe an individual's right to inspect, amend, and copy his PHI, and to receive an accounting of the uses and disclosures of his PHI during the last 6 years. It must also describe the individual's right to request restrictions on certain uses and disclosures of his PHI. 45 CFR § 164.520(b)(1)(iv).

√ *Complaint Procedures*

The Privacy Notice must include a statement that an individual who feels that his PHI has been improperly used or disclosed may file a complaint with the plan or the *Department of Health and Human Services* (DHHS). The notice must also state that the individual will not be retaliated against for filing a complaint. 45 CFR § 164.520(b)(1)(vi).

√ *Contact Information*

The Privacy Notice must contain the name, or title, and telephone number of the Contact Person. 45 CFR § 164.520(b)(1)(vii).

√ *Notice of Future Changes*

The Privacy Notice should warn participants that the plan's privacy policies may be modified in the future and that they will be notified of any changes. 45 CFR § 164.520(b)(3).

√ *Effective Date*

The Privacy Notice must contain the date on which the Notice is first in effect.

⇒ ***Plan Documentation***

Self-insured group health plans, by their very nature, require the involvement of the municipality in at least some plan administration decisions, which means that some employees of the sponsoring municipalities have access to PHI. In order to make sure that the use and disclosure of PHI is limited to the extent necessary and is not used for employment-based decisions or in connection with other benefit plans, the sponsoring municipality of any self-insured group health plan that covers at least 50 employees or that uses a TPA ***must certify*** to the plan that the ***plan documents have been amended*** to reflect the following new provisions, which focus on limitations and safeguards about the appropriate use and disclosure of PHI. 45 CFR § 164.504(f). Then, the municipality must agree to, and implement, the following procedures:

√ *Restricted Access to PHI*

The sponsoring municipality must identify the employees, classes of employees, or other persons under the control of the municipality that will be permitted access to PHI (including any individuals who might receive PHI in the ordinary course of business relating to the group health plan, such as auditors and benefits personnel), and then specifically restrict access to the identified individuals for the limited purposes of completing plan administrative functions. 45 CFR § 164.504(f)(2)(iii). Definition by job title is preferred.

√ *Permitted Use of PHI*

PHI should only be used and disclosed, as permitted by the plan document or as required by law. 45 CFR § 164.504(f)(2)(ii)(A). If feasible, all PHI received from the plan should be returned or destroyed when it is no longer needed. 45 CFR § 164.504(f)(2)(ii)(I). It is important to note, however, the municipality may freely keep information that it receives from other sources (such as the employee), or that it received prior to the effective date of the law, even if it would be PHI if it were received from the plan after the effective date of the Privacy Rule.

√ *No Use of PHI in Employment-Based Decisions*

The sponsoring municipality must not use or disclose PHI for employment-related decisions, or in connection with any other benefit or employee benefit plan that it sponsors. 45 CFR § 164.504(f)(2)(ii)(C). In addition, the sponsoring municipality must take steps to ensure that records maintained for the plan are adequately separated from records maintained for the municipality. 45 CFR § 164.504(f)(2)(ii)(J); 45 CFR § 164.504(f)(2)(iii). Again, information that a municipality obtains from a source outside the plan is not PHI.

√ *Reporting of Improper Use*

The sponsoring municipality must report any improper use or disclosure of PHI to the plan and develop a mechanism for resolving any noncompliance issues. 45 CFR § 164.504 (f)(2)(ii)(D).

√ *Participants' Access to PHI*

The plan must allow individuals to inspect, copy and amend PHI about themselves and must, upon request, provide an individual with an accounting of certain disclosures made of the individual's PHI by the plan or its business associates during the past 6 years. 45 CFR § 164.504(f)(2)(ii)(E)-(G); 45 CFR § 164.524; 45 CFR § 164.526; 45 CFR § 164.528.

√ *Federal Compliance Audit*

The plan must make its internal practices, books and records relating to the use and disclosure of PHI available to DHHS for purposes of auditing the plan's compliance with the Privacy Rule. 45 CFR § 164.504(f)(2)(ii)(H).

√ *Extension of Obligations to Contractors*

The plan must ensure that its agents and subcontractors will agree to abide by the same restrictions and conditions applicable to the municipality with regard to the use and disclosure of PHI received from the plan. 45 CFR § 164.504(f)(2)(ii)(B).

⇒ ***Contracts with Business Associates***

Municipalities sponsoring self-insured group health plans that cover at least 50 participants or use a TPA must review and amend the plan's service contracts with any business that is involved in the administration of the plan (*"business associates"),* to make sure that each business associate complies with the Privacy Rule, and to give the municipality the authority to unilaterally terminate the contract if the business associate does not comply. 45 CFR § 164.504(e)(i). (Note, however, that a business associate agreement is not required between the plan and the plan sponsor.) Many of these requirements closely parallel the obligations that are imposed on the sponsoring municipality itself, including:

√ The limited and proper use of PHI; document retention policies; and the reporting of any improper use or disclosure of PHI. 45 CFR § 164.504(e)(2)(i); 45 CFR § 164.504(e)(2)(ii)(A).

√ Procedures for permitting individuals to inspect, amend and obtain copies of their own PHI, and to receive an accounting of certain disclosures made of their PHI within the last six years. 45 CFR § 164.504(e)(2)(ii)(E)-(G).

√ The establishment of appropriate safeguards to prevent the improper use or disclosure of PHI. 45 CFR § 164.504(e)(2)(ii)(B).

√ Making its internal practices, books and records relating to the use and disclosure of PHI available to DHHS for purposes of auditing the plan's compliance with the Privacy Rule. 45 CFR § 164.504(e)(2)(ii)(H).

√ Making sure that all subcontractors of the business associate who handle PHI follow the Privacy Rule for the appropriate use and disclosure of PHI. 45 CFR § 164.504(e)(2)(ii)(D).

Compliance Issues For Municipalities That Sponsor Fully-Insured Group Health Plans

Municipalities that sponsor fully-insured group health plans are only required to comply with a limited number of requirements under the Privacy Rule, as long as ***two*** requirements are met:

(1) All of the health benefits must be provided to the municipality's employees through an insurance contract with a health insurance issuer or with an HMO;

and

(2) The group health plan must not create or receive PHI, except for information about enrollment and disenrollment, or summarized health information about aggregate utilization, benefits, and rates, which can be used for purposes of renewal bids, or evaluating whether to amend or terminate the plan.

45 CFR § 164.530(k). If these two requirements are met, it is presumed that the insurance company is the party that is creating or receiving the PHI, and the municipality sponsoring the fully-insured plan has only limited obligations, as follows:

√ *Establish a Policy Against Retaliation*

The sponsoring municipality must develop and implement a policy stating that it will impose sanctions and disciplinary action against any member of its workforce who intimidates or retaliates against individuals who exercise their rights under the Privacy Rule. 45 CFR § 164.530(g).

√ *Review Enrollment Materials*

All enrollment materials for the fully-insured group health plan should be reviewed to ensure that the plan does not require an individual to waive his rights under the Privacy Rule as a condition of enrollment or eligibility for benefits. 45 CFR § 164.530(h).

Note, however, that if a municipality sponsoring a fully-insured group health plan receives PHI from the plan, or from the insurance company or HMO, which is more than just enrollment, disenrollment, or summarized health information, then it will need to implement all of the administrative procedures, plan documentation, and certification standards that are imposed on municipalities sponsoring self-insured group health plans, as described above, and it will need to provide notices upon request. The cost of such compliance is substantial.

Compliance Issues For Municipalities That Provide On-Site Health Care

Although a municipality's on-site medical facility or program may not constitute a group health plan, it may be a *health care provider* under the HIPAA regulations. Health care providers will be considered a *"covered entity"* that must comply with the Privacy Rule if they conduct certain transactions electronically, or if they engage business associates to process such transactions electronically. 45 CFR § 160.103. In addition, the municipality's facility or program will have to comply with the electronic transaction standards and code sets for certain covered transactions. 45 CFR § 162.923.

If the municipality's on-site medical facility or other program does not conduct any of the specified transactions electronically, then it is not subject to the Privacy Rule. 45 CFR § 160.103.

Currently, the covered transactions that are subject to these electronic standards include:

√ *Health Claims and Equivalent Encounter Information*

Health care claims are requests by a provider to a health plan to obtain payment accompanied by the necessary information. If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of equivalent encounter information for purposes of reporting health care. 45 CFR § 162.1102

√ *Eligibility Inquiries*

Eligibility inquiries include inquiries from a provider or a health plan to a health plan concerning eligibility, coverage, and associated benefits under the applicable health plan, and the health plan's response to such an inquiry. 45 CFR § 162.1202.

√ *Referral Certifications and Authorizations*

Referral certifications and authorizations are requests or responses relating to authorizations for health care or referrals. 45 CFR § 162.1302.

√ *Status Inquiries*

Status inquiries involve questions about the status of a health care claim, and responses to those questions. 45 CFR § 162.1402.

√ *Enrollment and Disenrollment Information*

Enrollment and disenrollment information refers to subscriber enrollment information to a health plan, reflecting the subscriber's decision to establish or terminate insurance coverage. 45 CFR § 162.1502.

√ *Payment Information*

Payment and remittance information includes the transmission of information from a health plan to: (a) a health care provider's financial institution concerning payments made; information about the transfer of funds, or payment processing information; or the transmission of information; or (b) a health care provider, transmitting an explanation of benefits or remittance advice. 45 CFR § 162.1602.

√ *Premium Information*

Premium information includes the transmission by a responsible party to a plan of: (a) payment; (b) information about transfer of funds; (c) detailed remittance information; or (d) payment processing information concerning payroll deductions, other group premium payments or associated group premium payment information. 45 CFR § 162.1702.

√ *Coordination of Benefits Information*

Coordination of benefits information involves the transmission of information from any entity to a plan, in order to determine relative payment responsibilities of the health plan for health care claims or payment information. 45 CFR § 162.1802.

√ *Other Information*

Other information transmitted electronically may also be covered, including information regarding the first report of an injury, as well as health claims attachments, but standards for those transmissions have not been developed yet.

Electronic transmissions include transmissions over the Internet, Intranet, leased lines, dial-up lines, and private networks. It also includes those transmissions that are physically moved from one location to another using magnetic tape, disk or compact disk media.

A MUNICIPALITY'S PRELIMINARY CHECKLIST FOR COMPLIANCE WITH HIPAA'S ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS AND PRIVACY RULE

What follows is a preliminary checklist that may prove useful for municipalities as they begin to analyze their obligations under HIPAA's administrative simplification requirements and Privacy Rule with regard to the group health plans which they sponsor and with regard to any on-site facilities or programs which are considered "health care providers" subject to the Privacy Rule.

STEP #1: ⇒ **Identification**

- √ Identify all group health plans that are subject to HIPAA (such as medical plans, dental insurance, vision plans, medical flexible spending accounts, and employee assistance plans)

- √ Identify which plans are self-insured, covering more than 50 participants or using a third-party administrator, and therefore are subject to the HIPAA Privacy Rule

- √ Identify which plans are fully-insured and therefore may by subject to limited obligations under the HIPAA Privacy Rule

- √ Identify all non-health plans and benefits with access to PHI (such as life insurance, disability insurance, worker's compensation, and FMLA leave policies)

STEP #2 ⇒ **Analysis**

- √ Analyze the compliance obligations for each plan, depending on whether the plan is self-insured or fully-insured; the extent to which the plan creates or receives PHI; and the extent to which the municipality receives PHI from the plan or any administrator, insurance company, or HMO

STEP #2 ⇒ **Analysis** ***(continued)***

For each fully-insured plan

√ Evaluate whether the plan creates or receives only limited protected health information (*PHI)*, such as information about enrollment/disenrollment and summary health information, or whether it receives broader PHI, and whether the plan (or insurance company or HMO) discloses only such limited PHI to the sponsoring municipality

♦ *If only limited PHI (or less) is created or received by the plan and disclosed to the sponsoring municipality:*
→ Develop and implement a policy prohibiting retaliation against those individuals exercising their privacy rights
→ Review enrollment materials to make sure that the plan is not requiring that privacy rights be waived as a condition to enrolling in the plan or receiving benefits

♦ *If the plan creates or receives and discloses (or permits the insurance company or HMO to disclose) to the sponsoring municipality broader PHI:*
→ Comply with standards established for self-insured plans
→ Allocate privacy responsibilities among the municipality, insurer and any third parties

For each self-insured plan that covers at least 50 participants or that uses a third-party administrator

√ *Implement administrative policies and procedures on behalf of the plan*
♦ Develop an overall HIPAA privacy policy
♦ Appoint a "Privacy Official" and "Contact Person"
♦ Train appropriate personnel in privacy policies and practices
♦ Establish procedures for participants to inspect, amend and receive their PHI and receive an accounting of certain disclosures during the last 6 years
♦ Establish and implement a document retention policy, which will track disclosures of PHI
♦ Design and implement technical and physical safeguards for securing PHI
♦ Develop a complaint and grievance process, which will document all complaints received, and their disposition, if any

STEP #2 ⇒ **Analysis** ***(continued)***

For each self-insured plan that covers at least 50 participants or that uses a third-party administrator

√Prepare and distribute to participants a "Notice of Privacy Practices", on behalf of the plan
♦ Summarizing the rights of participants to PHI and the plan's obligation to protect it
♦ Describing the rights of participants to inspect, amend and receive copies of their PHI and of certain disclosures made of their PHI during the last 6 years

√Amend plan documents and certify that amendments have been made and implemented
♦ Amendments describing the permitted and required uses and disclosures of PHI
♦ Certification from sponsoring municipality that the plan document has been amended to limit the use of PHI and to erect firewalls to ensure the adequate separation of records between the group health plan and the municipality so that PHI is not used improperly

√On behalf of the plan, erect the firewalls described in the amended plan documents and plan certification
♦ Identify the individuals involved in the administration of the benefit plan and the receipt of PHI
♦ Establish policies so that PHI is provided, used, and disclosed only to the extent necessary to perform plan administrative functions
♦ Create adequate separation between PHI and other business and personnel information
♦ Implement training for designated workers and establish policies imposing sanctions and disciplinary measures for failure to follow Privacy Rule

√Review contracts with business associates
♦ Identify third parties or service providers who are "business associates"
♦ Review each contract
♦ Amend each contract, as necessary, to limit the use and disclosure of PHI; to impose similar requirements on business associates that are imposed on the municipality, and also to impose those requirements on the subcontractors of the business associates; to provide the municipality with the ability to unilaterally terminate the contract if the HIPAA Privacy Rule is not complied with; to provide that the municipality will be indemnified against any damages or losses that it may incur as a result of the failure of the business associate (or its subcontractors) to comply with the HIPAA Privacy Rule; and to include other requirements.

Step #3: ⇒ **Authorization**

- √ Prepare a sample authorization to be signed by employees, permitting the disclosure of their PHI for employment-related medical testing and non-health benefits (such as life insurance, disability insurance, workers' compensation, and FMLA), in accordance with municipal policy

Step #4: ⇒ **Review on-site medical services and other programs**

- √ Identify all on-site medical staff and health care services
- √ Determine if one or more "covered transactions" is conducted electronically.
  - √ If not, municipality will not be a health care provider subject to HIPAA Privacy Rule and standards for electronic transmissions of information
  - √ If so, comply with HIPAA's administrative requirements, Privacy Rule, and standards on electronic transactions

FAQs: FREQUENTLY-ASKED QUESTIONS ABOUT MUNICIPALITY OBLIGATIONS UNDER HIPAA'S PRIVACY RULE

Summarized on the following pages are some frequently-asked questions about HIPAA's administrative simplification requirements and the Privacy Rule which apply to municipalities, and answers to those questions.

FAQs and Answers

Scope of the HIPAA Privacy Rule

1. *Which benefit plans sponsored by a municipality are generally considered group health plans that are subject to HIPAA's Privacy Rule?*

   Medical, dental and vision plans and medical flexible spending accounts are generally considered group health plans and, therefore, ***are*** subject to the HIPAA Privacy Rule. The requirements are greater for group health plans which are self-insured and which cover at least 50 participants or which use a third-party administrator. 45 CFR § 160.103.

   In contrast, group-term life insurance, short-term disability, long-term disability and workers' compensation plans ***are not*** considered group health plans. 45 CFR § 160.103.

   Unlike many regulations which exempt governmental plans from the rules that apply to the private sector, the HIPAA Privacy Rule covers municipal, state and federal plans, even those self-funded non-federal governmental plans that are permitted to "opt out" of HIPAA's portability requirements.

2. *Are employee assistance plans ("EAPs") subject to HIPAA's Privacy Rule?*

   An employee assistance program ***may be*** considered a group health plan, subject to HIPAA's Privacy Rule, depending upon how it is structured. If the program provides direct treatment and counseling for medical conditions, as opposed to merely providing referrals, it may qualify as a group health plan. 45 CFR § 160.103.

3. *How can I tell if my health plan is a "small" health plan that can take advantage of the automatic one-year extensions for compliance with HIPAA's electronic standards requirements, medical privacy rules, and security standards?*

   HIPAA regulations state that a "small" health plan is a health plan with annual receipts of $5 million or less. 45 CFR § 160.103. In informal guidance, DHHS has stated that a fully-insured plan should look at the amount of premiums it paid

during its last full fiscal year, while a self-insured plan should look at the amount of medical claims reimbursed during its last full fiscal year. CMS HIPAA FAQ #4, issued 9/09/02; http://www.cms.hhs.gov/hipaa/hipaa2. A hybrid plan (one that has both self-insured and fully-insured components) should combine both the amount of premiums paid and the amount of claims reimbursed to determine whether the $5 million threshold has been reached. CMS HIPAA FAQ #4 issued 9/09/02; http://www.cms.hhs.gov/hipaa/hipaa2. Stop-loss premiums and administrative fees should not be counted. CMS HIPAA FAQ #38, issued 9/18/02; http://www.cms.hhs.gov/hipaa/hipaa2.

Uses of PHI Under the HIPAA Privacy Rule

1. *Can a municipality's group health plan automatically disclose PHI to another benefit plan, such as its group-term life insurance, short-term disability or long-term disability plan, to help determine an employee's eligibility for a benefit under one of those plans?*

   No, not without the employee's signed "*authorization*." 45 CFR § 164.508. To be valid under the HIPAA Privacy Rule, an authorization must meet certain specific criteria, including a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion; the name (or class of persons) to whom the information will be disclosed; a description of each purpose of the requested use or disclosure; statements about the employee's right to revoke an authorization; a statement that treatment, payment, enrollment or eligibility for benefits may not be conditioned on obtaining an authorization; and the expiration date of the authorization. 45 CFR § 164.508(b). An employee can withdraw this authorization.

2. *Does the HIPAA Privacy Rule prohibit a supervisor from receiving information about an employee's health from the employee?*

   No. The HIPAA Privacy Rule only restricts the flow of information from a covered entity, such as a municipality's group health plan, to the municipality. It does not prohibit the direct flow of information between employees and municipalities. 45 CFR § 164.501.

3. *Can a municipality use information about an employee's medical condition to defend itself in litigation where such information is germane?*

   Yes. However, if the information is supplied by the municipality's group health plan, a written authorization, meeting the standards for authorizations under the HIPAA Privacy Rule, must have been obtained. Alternatively, the HIPAA Privacy Rule does permit an individual's PHI to be disclosed in judicial proceedings, pursuant to a subpoena or discovery request, as long as certain requirements are met. 45 CFR § 164.512(e).

Administrative Procedures and Requirements

1. *Can any employee of the municipality serve as the HIPAA Privacy Official?*

   Yes. Unlike the Federal regulations that limit who can review adverse benefit determinations under group health plans, the HIPAA Privacy Rule does not place restrictions on who can serve as the plan's HIPAA Privacy Official. 45 CFR § 164.530(a).

2. *Can more than one person be designated as the HIPAA Contact Person?*

   Yes. The regulations permit an office – such as the HR or Benefits Office – to function as the Contact Person or office. 45 CFR § 164.530(a).

Impact of HIPAA Privacy Rule on Employment Practices

1. *Under HIPAA's Privacy Rule, can a municipality still require an applicant or employee to undergo pre-employment or active employment testing, respectively, such as drug testing and fitness-to-work assessments?*

   Yes, but the health care provider performing the testing will need the individual's authorization to release the results to the municipality, and the municipality will still need to comply with the standards imposed by the Americans with Disabilities Act and other relevant law. Nothing in the HIPAA Privacy Rule prohibits the municipality from conditioning employment on an individual signing the appropriate authorization. 45 CFR § 164.508.

2. *May a municipality's personnel or benefits department help employees with a claim dispute that the employee might have with the group health insurer?*

   Yes, a municipality's personnel or benefits department are free to advocate on behalf of employees as long as the plan does not provide the municipality with PHI without first obtaining the employee's authorization. 45 CFR § 164.506; 45 CFR § 164.508.

3. *Does the HIPAA Privacy Rule have an impact on the provision of on-site medical assistance, disease management activities, or other similar health improvement programs, such as preventive medicine, health education services and health risk assessments?*

   Maybe. Although these programs may not constitute group health plans, the underlying facility/providers may be subject to HIPAA's Privacy Rule if they conduct certain transactions electronically, such as communications regarding billing, payment, coordination of benefits, enrollment and disenrollment and eligibility. 45 CFR § 160.103.

Compliance Steps for Municipalities

1. *What must a municipality that sponsors a self-insured group health plan with at least 50 employees or a third-party administrator do in order to comply with the HIPAA Privacy Rule?*

   The municipality must, among other things:

   √ Develop, on behalf of the plan, a privacy policy addressing the privacy of PHI, document retention procedures, and a complaint/grievance process

   √ Appoint, on behalf of the plan, a Privacy Official and Contact Person

   √ Establish, on behalf of the plan, procedures for participants to inspect, amend and receive their PHI and an accounting of its disclosure

   √ Train appropriate personnel who may receive PHI on behalf of the plan about the plan's privacy policies and practices

   √ Develop sanctions against members of its workforce who fail to comply with the privacy policies and procedures

   √ Design and implement, on behalf of the plan, technical and physical safeguards for securing PHI

   √ Establish firewalls so that PHI is adequately separated from other employment and business records—this includes designating individuals who are authorized to receive PHI from the plan, training them, and establishing sanctions if the Privacy Rule is not followed

   √ Review enrollment materials to make sure that the plan does not require individuals to waive their rights under HIPAA's Privacy Rule as a condition of enrollment or eligibility for benefit.

   √ Amend its group health plan to incorporate privacy obligations, and provide the plan with a certification to that effect

   √ Prepare and distribute, on behalf of the plan, a Notice of Privacy Practices to plan participants

   √ Prepare, on behalf of the plan, a form authorization for use by participants

   √ Review and amend contracts with business associates to be sure that they also comply with the HIPAA Privacy Rule. The compliance deadline for this task may be extended under certain circumstances. Even if extended, however, the plan is not relieved of its obligations with respect to PHI held

by its business associates and has an affirmative duty to mitigate any harm caused by its business associates.

2. *Is there any way for a municipality to mitigate the burden of complying with the HIPAA Privacy Rule?*

The significant start-up and ongoing financial burden of complying with the HIPAA Privacy Rule may be largely avoided if a municipality provides health benefits to its employees by sponsoring a fully-insured group health plan, rather than a self-insured plan. However, this must be balanced against the flexibility and cost savings that many large municipalities enjoy by self-funding their health benefits rather than by providing fully-insured health insurance plans.

Liability, Penalties and Enforcement

1. *Who will administer and enforce the HIPAA Privacy Rule?*

The Office of Civil Rights of the U.S. Department of Health and Human Services (*"DHHS")* will administer and enforce the HIPAA Privacy Rule. 45 CFR § 160.300.

2. *What are the penalties for violating the HIPAA Privacy Rule?*

If you are a "covered entity" and you fail to comply with the HIPAA Privacy Rule, you may face a penalty of $100 for each violation, with the total exposure of no more than $25,000 for all violations of an identical requirement. 42 USC § 1320d-5.

If you knowingly violate the HIPAA Privacy Rule in your use and disclosure of PHI, fines can range from $50,000 to $250,000 and/or imprisonment of up to one year, five years, or ten years, depending on the circumstances of the use or disclosure. 42 USC § 1320d-6.

3. *Can an individual sue in a private right of action, if he thinks that he has been harmed by the improper use or disclosure of PHI?*

At this time, there does not appear to be a private right of action under the HIPAA Privacy Rule (although there may be rights under state privacy law). However, any person who believes that a covered entity is not complying with the privacy rules may file a complaint with DHHS.

4. *Is a group health plan liable for its business associate's violations of the HIPAA Privacy Rule?*

Not generally. However, if a plan knows of a pattern of activity or practice of the business associate that violates the Privacy Rule, it must take reasonable steps to cure the breach or end the violation. 45 CFR § 164.504(e)(2)(ii)(I). If these steps are unsuccessful, it must terminate the contract or, if it is not feasible to terminate the contract, report the problem to DHHS. 45 CFR § 164.504(e)(2)(iii). A plan may wish to protect itself from this potential liability by making sure that each of its contracts with a business associate provides that the business associate will indemnify the plan for any damages or financial losses that the plan (or the sponsoring municipality) incurs as a result of the business associate's failure to comply with the HIPAA Privacy Rule.