MUNICIPALITIES AS HYBRID ENTITIES UNDER HIPAA

by C. Michael Bakewell

In an age when people can share information with mass audiences in an instant, privacy can be challenging to protect. While this applies to many fields, healthcare is a top concern for the protection of confidential records. This article addresses the expectation of municipalities to comply with HIPAA requirements and ways to protect the health information of citizens without undue burden to local government services.

Risks of HIPAA Noncompliance By “Covered Entity” Municipalities

A municipality that qualifies as a “covered entity” under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must comply with the requirements of HIPAA for the protection of protected health information (PHI).

For municipalities, two possible functions may make the governmental entity a HIPAA “covered entity”: (1) a health plan and/or (2) a health care provider that electronically transmits health information in connection with a HIPAA transaction.

If a municipality or other governmental entity performs “covered entity” functions, then it is beyond debate that the governmental entity should comply with the HIPAA Privacy Rule and the HIPAA Security Rule. The penalties for noncompliance can be significant. For instance, in July 2011, the Health System of the University of California in Los Angeles resolved a HIPAA investigation with the United States Department of Health and Human Services (HHS) by agreeing to pay $865,500.00 for alleged employee violations of HIPAA. Among other changes, the HITECH Act increased the fines for noncompliance or violations of HIPAA occurring after Feb. 18, 2009. In Oct., 2009, the secretary of HHS issued its final interim rule for HIPAA enforcement and civil fines in accordance with the HITECH Act. Under this Interim Final Enforcement Rule, the amount of the civil penalties is based on the degree of a “covered entity’s” culpability, and has a dollar limit on identical violations occurring within a calendar year. The yearly limit, however, only applies to identical violations of the same HIPAA provision. The chart below, taken from the Interim Final Enforcement Rule, summarizes the increased civil penalties.

Of concern to a non-compliant municipality should be the announcement by the Office for Civil Rights of the U.S. Department of Health and Human Services in November 2011, that it was commencing random compliance audits of covered entities as required by the HITECH Act. The pilot audit program will perform 115 audits of “covered entities” within one year to assess privacy and security compliance. The HHS website provides information about who may be audited (every covered entity and business associate is eligible for an audit) and how the audit program will work. Recently, the Office for Civil Rights of HHS released its audit protocol. The audit protocol contains the requirements that auditors will review and assess in the audit process to analyze processes, controls, policies and procedures a “covered entity” has in place for HIPAA compliance. The audit protocol contains 77 performance criteria for Security Rule compliance and 88 performance criteria for Privacy Rule and breach notification requirements.

Civil Penalties for HIPAA Violations by Covered Entities and Business Associates

<table>
<thead>
<tr>
<th>Culpability for Violation</th>
<th>Per Violation</th>
<th>Maximum for Identical Violation of same HIPAA provision per calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect—corrected in timely manner</td>
<td>$10,000 up to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect—not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

In early 2009, Congress passed and the President signed the Health Information Technology for Economic and Clinical Health Act (HITECH Act) that enacted a number of changes to HIPAA. Among other changes, the HITECH Act increased the fines for noncompliance or violations of HIPAA occurring after Feb. 18, 2009. In Oct., 2009, the secretary of HHS issued its final interim rule for HIPAA enforcement and civil fines in accordance with the HITECH Act. Under this Interim Final Enforcement Rule, the amount of the civil penalties is based on the degree of a “covered entity’s” culpability, and has a dollar limit on identical violations occurring within a calendar year. The yearly limit, however, only applies to identical violations of the same HIPAA provision. The chart below, taken from the Interim Final Enforcement Rule, summarizes the increased civil penalties.

Of concern to a non-compliant municipality should be the announcement by the Office for Civil Rights of the U.S. Department of Health and Human Services in November 2011, that it was commencing random compliance audits of covered entities as required by the HITECH Act. The pilot audit program will perform 115 audits of “covered entities” within one year to assess privacy and security compliance. The HHS website provides information about who may be audited (every covered entity and business associate is eligible for an audit) and how the audit program will work. Recently, the Office for Civil Rights of HHS released its audit protocol. The audit protocol contains the requirements that auditors will review and assess in the audit process to analyze processes, controls, policies and procedures a “covered entity” has in place for HIPAA compliance. The audit protocol contains 77 performance criteria for Security Rule compliance and 88 performance criteria for Privacy Rule and breach notification requirements.
HHS is serious about HIPAA compliance by “covered entities.” For instance, the director of the Office for Civil Rights (OCR) has stated, as part of several HIPAA violation settlements, “We hope that health care providers … understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity.”19 “[W]e expect organizations to comply with their obligations under those rules regardless of whether they are private or public entities.”20

To avoid costly penalties for non-compliance, a municipality performing “covered entity” functions should thoroughly assess existing policies and procedures and use the OCR’s audit protocols as guidelines to conduct another risk assessment and ensure current compliance with the HIPAA Privacy and Security Rules.

why choose hybrid entity status

The HIPAA Privacy Rule permits an entity, such as a municipality, to separate its “covered entity” functions from its “non-covered entity” functions so that only the “covered entity” functions are required to comply with the HIPAA regulations.21 The separation of HIPAA-governed functions creates what is known as a “hybrid entity.” A municipality that performs “covered entity” functions should consider “hybrid entity” designation so that its departments that possess medical information on citizens, but do not perform “health plan” functions or “medical provider” functions, will not be required to protect that medical information in compliance with HIPAA.

If a governmental entity constitutes a “covered entity” or performs a “covered entity” function and has not made a hybrid entity designation, then the entire entity, including all of its departments, is required to comply with HIPAA.22 For example, (1) the police department, that generally does not perform “covered entity” functions, would have to secure and protect incident reports containing medical information under HIPAA; (2) the city jail, if it dispenses medication or has a notation referring to a prisoner’s medical condition, would have to comply with HIPAA; (3) a city utility with a “non-disconnect” customer list containing the customers’ medical conditions would be required to comply with HIPAA; or (4) the emergency dispatch (911) department (that dispatches police, fire and ambulance services) because it has data about the medical information of individuals would have to comply with HIPAA for all of its dispatching services.

By choosing hybrid entity status, a municipality may be able to reduce compliance costs and potential liability.

By choosing hybrid entity status, a municipality may be able to reduce compliance costs and potential liability. For instance, all workforce members of a covered entity are required to undergo training on HIPAA policies and procedures.23 Without a hybrid entity designation by a municipality, those employees who are unlikely to have any contact with PHI, such as building department employees, municipal court employees and street department employees, would still be required to receive initial and on-going HIPAA training. Similarly, a police department or jail that possesses individually identifiable medical information, as well as the employees of those departments, would be required to comply with HIPAA even if those departments perform no “covered entity” functions.

Without hybrid entity designation, a municipality and all of its departments would be required to perform extensive analyses, and adopt and implement a number of policies and procedures simply to ensure compliance with HIPAA. For example, the National Institute of Standards & Technology has issued a guide publication that contains approximately 40 pages of requirements, considerations, questions, analyses and policies for a covered entity to answer, review and implement just for compliance with the Security Rule.24 In addition, the HITECH Act adopted notice requirements that must be followed if a covered entity uses or discloses PHI in violation of HIPAA and its regulations.25 Those requirements include notifying the affected individual, as well as notifying HHS (and possibly the media), of the breach of PHI.26 Since 2009, over 430 entities have reported breaches of PHI to the U.S. Department of Health and Human Services that affect more than 20 million individuals.27 By adopting hybrid entity status, non-covered entity departments possessing individual health care information would not be subject to those notification requirements for a breach of PHI under HIPAA,28 and would not otherwise be required to comply with the HIPAA regulations.

Qualifying As A Hybrid Entity

To qualify for hybrid entity status, a governmental entity must be a single legal entity that performs both HIPAA-covered and non-covered functions.29 Hybrid entity status, however, is not automatic for a municipality meeting this definition. To become a hybrid entity, the governing body of the municipality must designate in writing those health care components and functions that must comply with HIPAA.30 This written designation must include all of those health care components that would meet the definition of a covered entity if those components were separate legal entities.31 With a hybrid entity...
designation, compliance with HIPAA only applies to the designated health care components; although, the municipality as a whole is still responsible for oversight, compliance and enforcement obligations.

A hybrid entity designation also permits the governmental entity to include in its list of designated health care components the functions of other departments not performing HIPAA-covered functions, but that do perform support activities for the health care components (e.g., those components that act as business associates for the health care components). For example, if the City’s finance department performs ambulance billing and is its only “covered” function, then only that function of the finance department could be included as a health care component in the hybrid entity designation. Thus, medical information collected in other functions of the finance department (such as the medical condition of customers on the “non-disconnect” list for the city-owned utility) would not be subject to HIPAA. Since the HITECH Act requires compliance by business associates with most provisions of the HIPAA Privacy Rule and Security Rule, a governmental entity declaring itself a hybrid entity may wish to consider including the portion of departments performing business associate functions as part of its health care components designation.

**Implementing The Hybrid Entity Designation**

Making a hybrid entity designation comes with its own set of compliance requirements. Once a municipality designates its “health care components” and “health care” functions as part of its hybrid entity designation, the municipality must implement certain policies and procedures as a hybrid entity. These include the following:

1. The municipality must create firewalls between its various health care components and between those components and non-HIPAA components. HIPAA prohibits one health care component from sharing PHI with another health care component or with a non-health care component if the disclosure would be prohibited by HIPAA where the components are separate legal entities.

2. The municipality must ensure that its designated health care components perform required risk analyses; develop and adopt appropriate policies and procedures; and train the affected workforce members for compliance with the HIPAA Privacy Rule and HIPAA Security Rule.

Consequently, with hybrid entity status, the governmental entity must develop clear policies, with sufficient training of affected employees, to ensure that PHI is not improperly shared or improperly used within the entity. Nonetheless, a municipality correctly designating its health care components and specific functions of departments that support those health care components can reduce its initial and on-going compliance costs and likely reduce its liability exposure by exempting a number of employees and operations from the requirements of HIPAA.

**Conclusion**

HIPAA compliance is essential for municipalities that perform “covered entity” functions as defined in the regulations. Because of the variety of services and functions typically provided by a municipality, HIPAA compliance, if required, poses substantial burdens and challenges. With the likely savings of time, expense and paperwork by declaring itself a hybrid entity, such a designation is worth consideration by a “covered entity” municipality.

C. Michael Bakewell practices law in the greater St. Louis area and is a graduate of the University of Missouri-Columbia School of Law. He has represented fire protection districts for over 20 years, and has advised several fire protection districts and private medical practices in achieving and maintaining compliance with HIPAA privacy and security regulations. Bakewell is a member of Barken & Bakewell, LLC and can be reached at 314-219-7554.

*You may request a copy of the footnotes for this article by calling Missouri Municipal League at 573-635-9134 or email info@mocities.com.*