HIPAA's Privacy and Security Rules and Their Effect on Local Governments

— by Juliana Reno and Joseph Lauber —

The Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) continues to affect municipalities in many ways. HIPAA has spawned detailed regulations known as the Privacy Rule and the Security Rule.[2] Most entities covered by HIPAA ("covered entities") had to comply with the Privacy Rule nearly two years ago. On April 25, 2005, covered entities will also be required to comply with the Security Rule.[3] This article will revisit some of the basic ways that the Privacy Rule applies to local governments, and will introduce the requirements of the Security Rule.

Municipalities as Covered Entities

A municipality must comply with HIPAA when it serves one of two functions: when it is a health care provider, or when it is the sponsor of a health plan.[4]

Many municipalities are health care providers. The scope of the term "health care provider" is quite broad. It includes not only hospitals and public clinics, but also, clinics in correctional facilities and ambulance services.[5] Significantly, however, HIPAA does not cover all health care providers — only health care providers who conduct certain electronic transactions are covered entities and subject to HIPAA.[6] Some municipal health care providers escape HIPAA's coverage because they do not conduct the specified electronic transactions. For example, some city jails dispense medication provided by the inmates or their families, but do not otherwise provide medical services. Generally, these jails do not submit bills to medical insurers, and they conduct all administrative tasks on paper, not online. Such a facility would probably not be a covered entity. In contrast, if a county operates a hospital, and seeks Medicare reimbursement for the services rendered (which Medicare requires to be in an electronic format),[7] the county qualifies as a covered entity. Likewise, if a city operates an ambulance service and submits bills to the insurance provider electronically, or receives payment through an electronic funds transfer, it is a covered entity.

A municipality must comply with HIPAA when it serves one of two functions: when it is a health care provider, or when it is the sponsor of a health plan.

Many municipalities are also health plan sponsors. A municipality "sponsors" a "health plan" if it offers its employees almost any sort of medical coverage or medical expense reimbursement. Sponsorship does not depend upon funding: a municipality sponsors a health insurance plan even if it requires its employees to pay the entire premium. Under the Privacy Rule, a "health plan" means not only health insurance, but also dental, vision, and prescription drug coverage.[8] "Health plan" also includes employee assistance plans (arrangements which provide counseling to employees and their families), and medical expense reimbursement arrangements, but does *not* include workers' compensation, short-term or long-term disability coverage, or life insurance.[9]

Like health care providers, health plans are covered entities and must comply with HIPAA. If a municipality's health plan is fully insured — if benefits are paid through an actual insurance contract — then the insurance company will be responsible for most (but not all!) HIPAA compliance tasks. However, if a municipality's health plan is self-insured, the municipality will bear primary responsibility for HIPAA compliance. In this context, medical expense reimbursement plans are considered self-insured plans.

Under both the Privacy Rule and the Security Rule, covered entities are required to safeguard various forms of protected health information, or PHI. PHI is individually identifiable health information that relates to a patient's condition, to the provision of care, or to the payment for medical services[10] — things like patient charts and records, medical bills, health care claims, and explanation of benefits. By regulation, PHI does not include records held by a covered entity in its capacity as an employer.[11] For example, if an employee brings in a doctor's note in order to document the need for sick leave, that note is not PHI. But a municipality must take care — the same note, if provided to the city's health plan administrator in order to document a health care claim, *is* PHI.

Privacy Rule Requirements

The Privacy Rule prohibits covered entities from using or disclosing PHI, except as specifically provided in the Privacy Rule.[12] Improper uses or disclosures of PHI, if unintentional, can result in civil penalties of $100 per violation (capped at $25,000 per year for

identical violations).[13] Intentional violations can result in criminal penalties of up to $250,000 per violation and ten years' imprisonment.[14]

In order to avoid improper use or disclosure, the Privacy Rule requires a covered entity to design and implement written privacy policies and procedures.[15] Among other things, the privacy policies and procedures must explain how PHI will be handled throughout the covered entity, and how violations of the policies and procedures will be addressed. The Privacy Rule also requires covered entities to respect and enforce certain individual rights recognized by HIPAA. For example, under HIPAA, an individual has the right to access his or her own PHI.[16] The Privacy Rule details matters such as the way in which requests for access should be made, the time frames for responding, and even the amount that can be charged for copies made upon such a request.[17] The Rule also elaborates upon an individual's right to receive a written notice explaining the covered entity's privacy policies,[18] and an individual's right to know what disclosures of his or her PHI the covered entity has made.[19]

A municipality can take steps to reduce its exposure to Privacy Rule liability and to reduce its HIPAA compliance burden. The simplest of these steps is known as a "hybrid entity designation." A hybrid entity is a single legal entity that has both covered and non-covered functions.[20] For example, a city is a single legal entity which may have both covered functions (clinics) and non-covered functions (a court system, snow removal facilities, or a water treatment plant). Because health plans are legal entities in their own right, a city is not a hybrid entity simply by virtue of sponsoring a health plan. However, a plan can be a hybrid entity if it offers both covered and non-covered benefits — for example, a cafeteria plan that offers both medical reimbursement (covered) and child care reimbursement (non-covered). A hybrid entity can choose to have HIPAA apply to all of its functions, or to have HIPAA apply only to its covered functions. To make the latter choice, the hybrid entity creates a written document — the hybrid entity designation — which identifies the covered and non-covered components, and which states that only the covered components will comply with HIPAA.[21]

Security Rule Requirements

In addition to Privacy Rule requirements, local governments will soon have additional HIPAA obligations.[22] Unlike the Privacy Rule, which is designed to keep covered entities from improperly disseminating PHI, the Security Rule seeks to ensure that those who are not authorized to obtain PHI cannot breach an entity's electronic recordkeeping system. The Privacy Rule keeps PHI from getting out to the unauthorized; the Security Rule keeps the unauthorized from getting in to the PHI.

While the Privacy Rule applies to all forms of PHI, the Security Rule applies only to one form — electronic PHI, or ePHI (PHI that is stored or transmitted electronically).[23] Because the Security Rule is limited to ePHI, most covered entities have found that compliance with the Security Rule involves different personnel than compliance with the Privacy Rule. For health care providers, Privacy Rule compliance is largely a matter for office managers, risk managers, medical records managers, and medical/legal compliance officers. For sponsors of health plans, Privacy Rule compliance is usually implemented by the human resources or benefits departments. In contrast, a covered entity should expect that Security Rule compliance will be mainly in the hands of an information technology or medical information systems department, or computer experts.

Although the Security Rule contains some very specific technical guidelines, the Security Rule also attempts to provide flexibility, so that a covered entity can comply with the rule within the context of the entity's size and technological capabilities.[24] In general, the Security Rule requires a covered entity to ensure the confidentiality, integrity and availability of all ePHI; to protect against reasonably anticipated threats to security and uses and disclosures of ePHI; and to ensure that its workforce complies with the Security Rule.[25]

The Security Rule contains thirteen mandatory implementation specifications and numerous "addressable" implementation specifications.[26] A covered entity must follow the mandatory implementation specifications. With regard to the addressable specifications, however, the entity must first determine whether each specification is a "reasonable and appropriate security measure" for the covered entity's own "particular security framework."[27] To make this determination, the covered entity must consider its own size, complexity and capabilities, its technical software capabilities, the cost of the specified security measures, the probability of potential security risks to ePHI, and how critical those risks are.[28] Based on its conclusion, the covered entity may implement the

continued on page 8

Juliana Reno, a partner at Stinson Morrison Hecker LLP, is a member of the Employee Benefits Practice Division. Her practice includes both transactional work and litigation. On the transactional side, Juliana works with both pension plans, and with health and welfare plans, on a variety of ERISA matters. In the courtroom, Juliana focuses on employment and ERISA litigation. Juliana has assisted municipalities with their HIPAA compliance efforts, both in the health plan arena and in the provider arena, for several years.

Joseph G. Lauber, an associate at Stinson Morrison Hecker LLP, is a member of the Public Law & Finance Practice Division. Joe has experience in general public and municipal law issues, including ordinance drafting, condemnation, annexation, Board of Zoning Adjustment matters, development code drafting and the effect of HIPAA on local governments.

addressable specification, implement an alternative measure, or do nothing, provided that the standard provided in the Rule can still be met.[29] Even if the covered entity determines that addressable specifications are not appropriate, the entity must still implement policies and procedures to ensure that the security standard is met — the implementation specifications are optional, but the security standards are not.

To comply with the Security Rule, covered entities must act to protect ePHI through the implementation of administrative, technical and physical safeguards.[30] As noted above, each type of safeguard contains several standards, and each standard contains several implementation specifications. The remainder of this article will provide some details concerning these safeguards, standards, and specifications. Please remember that HIPAA security is highly technical. There is no way for your authors to transform this material into a best-selling novel, or even a good read. That said, the basic outlines of the Security Rule are understandable even to the computer inept. We offer the following not as a detailed explanation of the Rule, but as a way for municipalities to become familiar with the basic ideas and terminology of the Security Rule.

Administrative Safeguards

There are eight administrative standards:

1. Security Management Process. Each covered entity must implement policies and procedures designed to "prevent, detect, contain, and correct security violations."[31] This standard has four required implementation specifications — a covered entity must conduct a risk analysis to assess potential risks and vulnerabilities of ePHI;[32] develop and implement risk management policies and procedures;[33] adopt sanctions against its employees who violate the security rule and apply those sanctions; and conduct regular reviews of activity in its information system.[34]

2. Assigned Security Responsibility. A covered entity must name a "Security Officer," the individual who will be responsible for the development and implementation of security policies and procedures.[35] The Security Officer focuses the covered entity on the importance Security Rule compliance.[36]

3. Workforce Security. All members of the covered entity's workforce should have appropriate access to ePHI, but employees who are not authorized to access ePHI should be prevented from obtaining it.[37] This standard contains three addressable implementation specifications, and in substance, each of these specifications is a strong suggestion that the covered entity may need to adopt procedures in specific areas. A covered entity must assess its need for procedures covering the authorization or supervision of employees working with ePHI; the method for determining which employees may access ePHI; and the termination of an employee's access to ePHI.[39]

4. Information Access Management. This standard makes access to ePHI subject to the "minimum necessary" standards established in the Privacy Rule.[39] Under the two applicable specifications, both of which are addressable, a covered entity must assess whether it needs policies and procedures to grant a user access to ePHI, and whether it needs policies and procedures for reviewing and modifying a user's continued ePHI access.[40]

5. Security Awareness and Training. The Security Officer must "implement a security awareness and training program for all members of its workforce."[41] A covered entity should assess its need for periodic security updates for protection from malicious software, for monitoring log-in attempts, and for password management procedures.[42]

6. Security Incident Procedures. A covered entity must formulate policies and procedures that address the occurrence of security incidents.[43] A security incident occurs when the entity suffers an attempted or successful unauthorized utilization of ePHI, or when the entity's system operations have been interfered with.[44] A covered entity must identify and respond to all suspected and known security incidents, must mitigate any harmful effect of a security incident, and must document each security incident and its outcome.[45]

7. Contingency Plan. A covered entity must establish a contingency plan, made up of policies and procedures to be followed in the event of an emergency or other occurrence which causes damage to the entity's systems containing ePHI.[46] There are three required implementation specifications to guide the entity's compliance with this standard — the covered entity must establish: a data backup plan to "create and maintain retrievable exact copies" of ePHI;[47] a disaster recover plan to restore any lost ePHI;[48] and an emergency operation plan, to continue the processes necessary to protect ePHI while the system is operating in emergency mode.[49] A covered entity must also assess its need to periodically test and revise its contingency plan, and its need to determine the applications and data which are critical to its contingency plan.[50]

8. Evaluation. A covered entity must perform a periodic evaluation of any operational changes that may have affected the entity's security policies and procedures.[51]

Physical Safeguards

There are four physical safeguard standards:

1. Facility Access. A covered entity must limit physical access to its electronic information systems and the areas in which they are located.[52] Covered entities must also ensure that only properly authorized individuals can physically access ePHI.[53] A covered entity should assess its need for governing facility access while an entity is operating under its disaster recovery plan or in emergency operations mode; making the entity's facilities and equipment safe from unauthorized access, tampering, and theft; validating an individual's access to facilities; and documenting the maintenance of the portions of the facility which relate to ePHI security.[54]

2. Workstation Use. For each workstation that has access to ePHI, a covered entity must specify the functions that can be performed, the manner in which they can be performed, and the physical surroundings of the workstation.[55]

3. Workstation Security. A covered entity must create physical safeguards to restrict workstation access, so that only authorized users can reach ePHI.[56]

4. Device and Media Controls. A covered entity must control the movement of hardware and electronic media that contain ePHI as they migrate into, through, and out of the facility.[57] Two mandatory implementation specifications apply under this standard: implementation of procedures governing the final disposition of ePHI and the hardware on which it is stored,[58] and governing the removal of ePHI from electronic media before the media are made available for re-use.[59] The covered entity must assess its need to establish a record of the movements of hardware and electronic media, and its need to create duplicate ePHI before moving equipment.[60]

Technical Safeguards

There are five technical safeguard standards:[61]

1. Access control. ePHI must only be accessible to those with proper authorization.[62] Unique user identifications and emergency access procedures are required.[63] A covered entity should assess its need for automatic log-off procedures and encryption.[64]

2. Audit controls. A covered entity must be able to track activity that occurs in any information system where ePHI is located.[65]

3. Integrity. ePHI must be protected from improper alteration of destruction.[66] A covered entity must assess its need to have mechanisms that can corroborate whether ePHI has been improperly altered or destroyed.[67]

4. Person or Entity Authentication. When an individual seeks access to ePHI, there must be some way to confirm the individual's identity.[68]

5. Transmission Security. A covered entity must have security measures which protect ePHI while it is being transmitted over an electronic communication network.[69] The covered entity should consider its needs for a process to confirm that ePHI was not modified during transmission, and its need for encryption.[70]

Conclusion

The goals of HIPAA are clearly praiseworthy. It is nearly impossible to argue against a uniform standard for protecting individual health information, or against an individual's right to access. At the same time, HIPAA imposes significant obligations on covered entities, including municipalities. Those obligations cannot be wished away — HIPAA is here to stay. Municipalities must determine the extent to which they are covered by HIPAA, take steps to limit their liability exposure and compliance burden, and then work diligently toward full compliance with HIPAA.

Notes

1. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).
2. 45 C.F.R. Parts 160, 162, and 164 (2003) (Security Rule) and 45 C.F.R. Parts 160 and 164 (2002) (Privacy Rule).
3. 45 C.F.R. §164.318 (2003).
4. *See* 45 C.F.R. §160.102 (2002).
5. 42 U.S.C. §1395x(5) (West 2005).
6. 45 C.F.R. §160.102(a) (2002).
7. 42 U.S.C. §1395y (West 2005).
8. 45 C.F.R. §160.103 (2003).
9. *Id.*
10. *Id.*
11. *Id.*
12. 45 C.F.R. §164.502 (2002).
13. 42 U.S.C. §1320d-5 (West 2005).
14. *See id.* §1302d-6.
15. 45 C.F.R. §164.530(I) (2002).
16. 45 C.F.R. §164.524 (2002).
17. *Id.*
18. *See* 45 C.F.R. §164.520 (2002).
19. *See* 45 C.F.R. §164.528 (2002).
20. 45 C.F.R. §164.103 (2003).
21. *See* 45 C.F.R. §164.105 (2003).
22. *See* 45 C.F.R. §164.318 (2003).
23. *See* 45 C.F.R. §164.302 (2003).
24. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8369 (Feb. 20, 2003).
25. *See* 45 C.F.R. §164.306(a) (2003).
26. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8369.
27. *See* 45 C.F.R. §164.306(d) (2003).
28. 45 C.F.R. §164.306(b)(2).
29. *See* 45 C.F.R. §164.306(d) (2003).
30. *See* 45 C.F.R. §§164.308 through 164.312 (2003).
31. 45 C.F.R. §164.308(a)(1) (2003).
32. *Id.*
33. *Id.*
34. *Id.*
35. 45 C.F.R. §164.308(a)(2) (2003).
36. *Id.*
37. 45 C.F.R. § 64.308(a)(3) (2003).
38. *Id.*
39. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8349 (Feb. 20, 2003).
40. *See* 45 C.F.R. §164.308(a)(4) (2003).
41. 45 C.F.R. §164.308(a)(5) (2003).
42. *Id.*
43. 45 C.F.R. §164.308(a)(6) (2003).
44. 45 C.F.R. §164.304 (2003).
45. 45 C.F.R. §164.308(a)(6) (2003).
46. 45 C.F.R. §164.308(a)(7) (2003).
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. 45 C.F.R. §164.308(a)(8) (2003).
52. 45 C.F.R. §164.310(a) (2003).
53. *Id.*
54. *Id.*
55. 45 C.F.R. §164.310(b) (2003).
56. *See* 45 C.F.R. §164.310(c) (2003) .
57. 45 C.F.R. §164.310(d) (2003).
58. *Id.*
59. *Id.*
60. *Id.*
61. 45 C.F.R. 164.312 (2003).
62. 45 C.F.R. §164.312(a) (2003).
63. *Id.*
64. *Id.*
65. 45 C.F.R. §164.312(b) (2003).
66. 45 C.F.R. §164.312 (c) (2003).
67. *Id.*
68. 45 C.F.R. §164.312(d) (2003).
69. 45 C.F.R. §164.312(c) (2003).
70. *Id.* ML