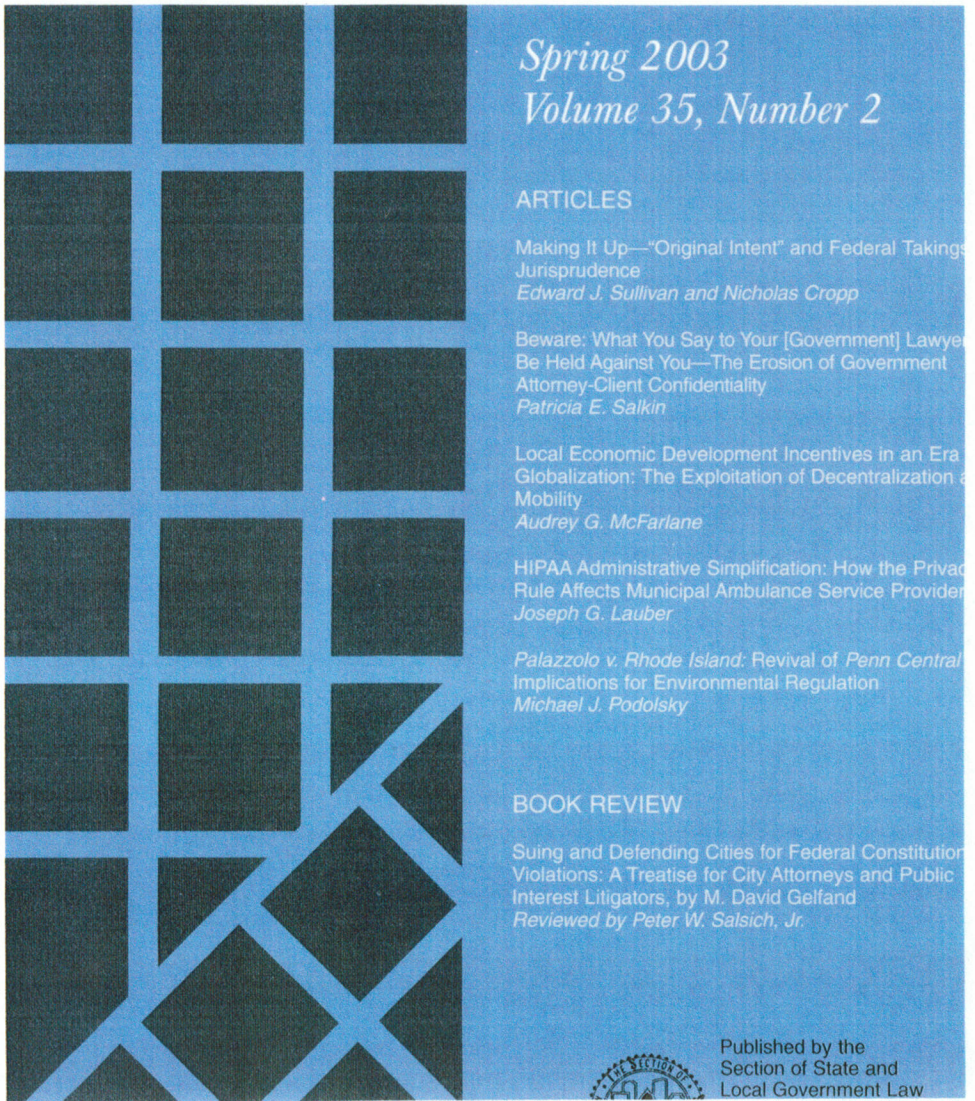
The Urban Lawyer

The National Quarterly Law Journal on State and Local Government Law



HIPAA Administrative Simplification: How the Privacy Rule Affects Municipal Ambulance Service Providers

Joseph G. Lauber*

I. Introduction

WHEN I THINK ABOUT the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its potential effect on municipal ambulance service providers, I am reminded of a conversation I had several years ago with a police officer friend who had assisted in the cleanup of the 1993 Catoosa, Oklahoma tornados. He explained that several fatalities occurred because one of the tornados was so large that motorists did not recognize what it was and simply drove into it.[1] Similarly, the sheer size of HIPAA may cause those entities that must comply with its provisions to blindly enter the HIPAA compliance period without taking precautions to protect against HIPAA liability. This article is designed to serve as a warning siren to municipalities that have not yet taken steps to become HIPAA compliant, and as a "HIPAA-safety action plan" for those that have. Special emphasis is placed on the privacy rule requirements for municipal ambulance service providers.

HIPAA is a colossal piece of legislation that is changing the way business is conducted in the health care industry. Due to its vastness, HIPAA can be very difficult to conceptualize: HIPAA is not simply a shift in the paradigm; it is a new and independent paradigm. Through the analysis in this article several points regarding HIPAA will become evident: First, HIPAA is enormous and likely applies to local governments in various ways. These government agencies should seek to obtain a general familiarity with HIPAA and how it may apply to them. Second, HIPAA applies to local governments that operate municipal ambulance services either now, because they are health care providers

*Joseph G. Lauber practices with the Public Law Practice Division at Stinson Morrison Hecker LLP, Kansas City; J.D., University of Missouri-Kansas City School of Law, 2003; B.B.A. University of Oklahoma.

1. Two tornadoes, each 250 yards wide, struck Catoosa on April 24, 1993. *See* http://www.srh.noaa.gov/oun/stormdata/okc9304.html (last visited Dec. 27, 2002). Most of the storm's seven fatalities were motorists driving along Interstate 44. *See* Samuel D. Barricklow, *April 23, 1993: The Killer Tornado in Tulsa, Oklahoma, available at* http://www.k5kj.net/930424.htm (last visited Dec. 27, 2002).

who transmit health information electronically, or will apply later, because they will be required to transmit billing to Medicare in the future.[2] HIPAA's application requires these covered entities to adjust the way they currently do business, both externally and internally, in many ways. Third, local governments that qualify as HIPAA-covered entities need to take action to become compliant with HIPAA because there can be severe consequences for noncompliance.

This article begins by summarizing the scope of HIPAA's multifarious provisions to set the proper context for the narrower discussion of the privacy rule and its effect on municipal ambulance companies. HIPAA requires municipal ambulance suppliers to develop policies and procedures that enable individuals to access their health information more easily, utilize standard information in the transfer of health information, and protect an individual's health information from unnecessary disclosure. This article summarizes the coverage of HIPAA's five titles. From this summation, the discussion shifts specifically to a detailed analysis of Title II: administrative simplification. Through its transaction and code sets rule, administrative simplification establishes standards that will make the exchange of information in health care industry transactions more efficient, both among the various organizations and to the individuals who are the subject of the data. With the increased fluidity of information, however, comes a fear that it will be easier than ever for private health information to leak out into the public domain. This article summarizes the resolution of these concerns through the provisions of the security rule, which compels HIPAA-covered entities to erect barriers to keep private health information from being taken from the entity, and the privacy rule, which requires covered entities to enact precautions to prohibit the disclosure of private health information outside the entity. After establishing a context of HIPAA's provisions, Part III examines the issues that arise when the privacy rule is applied to municipal ambulance service providers. Several legal questions are addressed, including how ambulance services qualify as HIPAA-covered entities, and how HIPAA affects state open record laws. Part IV offers an outline of the steps a municipal ambulance service provider should take to become HIPAA compliant. Finally, in Part V, this article provides an overview of how the Office of Civil Rights will enforce the privacy rule against the covered entities.

2. Administrative Simplification Compliance Act, § 3, Pub. L. No. 107–105, 2001 U.S.C.C.A.N. (115 Stat.) 1003 (to be codified at 42 U.S.C. § 1395y). In testimony before a United States Senate committee, a paramedic testified that in Minnesota one-half of the patients receiving ambulance service bill their payments through Medicare. *Testimony Before the Senate Committee on Governmental Affairs* (2001) (statement by Gary L. Wingrove, EMT-P, Paramedic and Manager at Minnesota Ambulance Association). In the eight years from 1987 to 1995, Medicare's payout to ambulance service providers went from $602 million to nearly $2 billion. *Ambulance Services: Changes Needed to Improve Medicare Payment and Coverage Decision Policies, Testimony Before the Senate Committee on Governmental Affairs* (2001) (statement by Laura A. Dummit, Director, Health Care- Medicare Payment Issues). This sharp increase stabilized at total payments of $2.1 billion over the next two years. *Id.*

II. HIPAA

A. *History and Background of HIPAA*

HIPAA, signed into law on August 21, 1996, by President Clinton, is widely recognized as the most sweeping legislation to affect health care in the United States since President Johnson approved Medicare in 1965.[3] HIPAA is the sole survivor of the Clinton Administration's failed attempts to overhaul the health care system in 1993 and 1994.[4] Despite the failure of President Clinton's health care program and the shift to a Republican majority in both Houses of Congress, HIPAA enjoyed overwhelming bipartisan support.[5]

Also known as the Kennedy-Kassebaum Act,[6] HIPAA was initially designed to address one particular issue that came to the forefront during the health care debates of the early nineties: retaining health insurance coverage for employees and their families (especially those with pre-existing conditions) when they lose or change their jobs.[7] Although HIPAA was both disappointing in its scope to liberals, who commented that HIPAA was "[b]etter than nothing,"[8] and criticized by conservatives as "letting in through the back door the very health care socialization . . . barred at the front door [in 1994],"[9] the Health Insurance

3. *See, e.g., HIPAA Compliance: What Leadership Role Should the State Have?* Background Paper for the California Senate Insurance Committee, Senate Health and Human Services Committee, and Senate Privacy Committee Joint Informational Hearing, May 16, 2001, *available at* http://www.sen.ca.gov/ftp/sen/committee/standing/insurance/info_hearings/backgrounds/5–16–01_hipaa_compliance.doc (last visited Dec. 30, 2002).

4. *See* Trudy Lieberman, *You Can't Take It with You,* COL. JOURNALISM REV. July-August 1997, *available at* http://www.cjr.org/year/97/4/medi.asp (last visited Dec. 26, 2002).

5. *See* Pete du Pont, *Kennedy-Kassebaum, the Revolution's Waterloo?,* National Center for Policy Analysis, April 18, 1996, *available at* http://www.ncpa.org/oped/dupont/keka.html (last visited Dec. 26, 2002). The Senate voted 98–0 to approve the Kennedy-Kassebaum Bill one day after the House passed it 421–2. Reuters Tuesday, August 6, 1996, *available at* http://www.amso.com/kassreuters.html (last visited Dec. 26, 2002).

6. Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat.) 1936.

7. *See* Lieberman, *supra* note 4.

8. Paul Starr, *The Signing of the Kennedy-Kassebaum Bill,* Aug. 22, 1996, *available at* http://www.princeton.edu/~starr/articles/signing.html (last visited Dec. 26, 2002).

9. du Pont, *supra* note 5.

Association of America and the American Medical Association hav both asserted the need for legislation of its genre.[10]

B. *Organization of HIPAA*

HIPAA is divided into five titles. Title I, Health Care Access, Portabilit and Renewability, generally enhances both the Employee Retiremer Income Security Act of 1974 (ERISA) and the Public Health Servic Act, to increase the portability of health insurance by limiting exclu sions that can be made for pre-existing conditions, prohibiting discrin ination based on claim history or health status, and guaranteeing th availability or renewability of health coverage for individuals with pric coverage.[11] Title II addresses the issues of preventing health care frau reform of medical liability, and administrative simplification.[12] Th title amends the Social Security Act and includes provisions to contr fraud and abuse in health plans, revisions to civil and criminal penaltie for health care fraud, coordination of Medicare-related health plans an measures to simplify the administration of health care in the Unite States.[13] Components of Title II will be the focus of this article, and fc that reason this portion of HIPAA will be addressed in more deta below. Some of the provisions found in HIPAA Title III are changes t the Tax Code, including the creation of a deduction for funds paid int Medical Savings Accounts (MSAs), increased deductions for the healt insurance expenses of self-employed individuals, shifting the treatmer of long-term care agreements as an insurance contract, and tax exemp tion for state insurance pools.[14] With provisions similar to those fc individuals covered in Title I, Title IV covers portability, access, an renewability for group health plans.[15] Title V addresses various revenu offsets.[16]

10. *See* Erik A. Carlson, *HIPAA to Bring Sweeping Changes Nationwide,* TH POST ONLINE EDITION, Sept. 30, 2002, *available at* http://thepost.baker.ohiou.ed archives3/sep02/093002/n3.html (last visited Dec. 30, 2002).

11. *See* Health Insurance Portability and Accountability Act of 1996, tit. I, Pub. I No. 104–191, 1996 U.S.C.C.A.N. (110 Stat.) 1939–91.

12. *See* HIPAA, tit. II, Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat 1991–2037.

13. *See id.*

14. *See* HIPAA, tit. III, Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat 2037–72.

15. *See* HIPAA, tit. IV, Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat 2073–89.

16. *See* HIPAA, tit. V, Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat 2089–2103.

C. *Administrative Simplification*

At its core, HIPAA's Title II is a series of regulations that make health care information easier for individuals to use and access, while it also creates safeguards to ensure that others cannot take advantage of the resulting simplification. HIPAA's administrative simplification provisions can be broken down into four basic parts: electronic health transaction standards, unique identifiers, security and electronic signature standards, and privacy and confidentiality standards.[17] The enumerated purpose of HIPAA's administrative simplification amendments to the Social Security Act is to "improve the Medicare program . . . of the Social Security Act, the medicaid program, . . . and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[18] Underscoring the need for uniform standards is the fact that the Department of Health and Human Services (HHS) estimates that there are currently more than 400 assorted formats for health insurance claims forms alone.[19] In fact, "[I]t is estimated that more than $.20 of every healthcare dollar is spent on administrative overhead, with an additional $.11 of every healthcare dollar spent fraudulently."[20] Conservative estimates suggest that the implementation of HIPAA will save health care providers $9 billion annually.[21]

Three major rules relating to HIPAA administrative simplification have been promulgated. The first of these is the transactions and code sets (TCS) rule.[22] The TCS rule is designed to simplify the exchange of information in the health care industry and generally sets forth standards for uniform data elements of health care transactions.[23] The second is the security rule proposed by the Department of Health and Human Services to address concerns over physical and technological safeguards to health information stored and exchanged in the health

17. Phoenix Health Systems, *HIPAA Primer: What Is HIPAA?, available at* http://www.hipaadvisory.com/regs/HIPAAprimer1.htm (last visited Jan. 2, 2003); *See also* HIPAA §§ 262–264 Pub. L. No. 104–191, 1996 U.S.C.C.A.N. (110 Stat.) 2023–34; 42 U.S.C. § 1320d-2 (2000).

18. HIPAA § 261, 42 U.S.C. § 1320(d) (2000).

19. Chris Tabatzky et al., *HIPAA: Headache or Headway?,* paper submitted to the Department of Preventive Medicine and Biometrics, Uniformed Services University of the Health Sciences, October 29, 2002, *available at* http://hsa.usuhs.mil/pmo526/papers/archaic5.pdf (last visited Dec. 30, 2002).

20. *Id.*

21. *Id.*

22. 45 C.F.R. pt. 162.

23. *See id.*

care system.[24] The third rule, the privacy rule, lists three major purposes: the protection and enhancement of health care consumers' rights by improved access to and controlled use of their health information, restoration of trust in the health care system, and the creation of a national framework for privacy protection.[25] Together, these three rules serve the function of simplifying the exchange of information in the health care industry and improving the ease with which an individual can access the information that is created about them for use in health care. Simultaneously, these rules operate to prevent an adverse secondary effect of this simplification: the fact that it will also be easier than ever for others to access private health information.

1. ELECTRONIC HEALTH TRANSACTIONS STANDARDS

Although this article is specifically designed to address the effect of the privacy rule on municipal ambulance service providers, the transactions and code sets rule ("TCS rule")[26] is an important component in the larger HIPAA compliance picture. It is critical for entities covered under HIPAA to understand that the TCS rule provisions will constitute a significant portion of their compliance plan and, if the provider is not already required to comply with the TCS rule, they will be by October 16, 2003.[27] As a result, additional detail is provided in the summary of TCS rule requirements that follow.

Initially, HIPAA sets out to accomplish its purpose of improving health care efficiency by requiring the Secretary of Health and Human Services to adopt uniform standards for the electronic exchange of health information.[28] These "electronic health transactions" include health plan eligibility information, enrollment and disenrollment, claims, and premium payments.[29] Rules that address first injury reports and health claims attachments are forthcoming.[30] Notwithstanding a few exceptions, standards must be developed by an American National Standards Institute (ANSI) accredited organization.[31] The Department of Health and Human Services published the final TCS rule on August

24. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified in scattered sections of 45 C.F.R. pts. 160 and 164).
25. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000).
26. 45 C.F.R. pt. 162.
27. *See* Administrative Simplification Compliance Act, § 2, 42 U.S.C.A. § 1320d-4.
28. 42 U.S.C.A. § 1320d-2.
29. Phoenix Health Systems, *supra* note 17.
30. Phoenix Health Systems, *Guide to Transactions and Code Sets Standards, available at* http://www.hipaadvisory.com/action/Compliance/Trans-CodeSetsGuide.htm (last visited Jan. 4, 2003).
31. 42 U.S.C.A. § 1320d-1(c)(1).

17, 2000.[32] Except for small health plans,[33] HIPAA-covered entities were required to comply with the TCS rule by October 16, 2002.[34]

"Covered entities" are the types of businesses that are affected most by HIPAA because its requirements will apply to them directly. There are three types of entities to which the provisions of HIPAA apply: health plans, health care clearinghouses, and health care providers.[35] Note, however, that although plans and clearinghouses are covered regardless of how they transmit information, only those health care providers that transmit health information in electronic form in connection with a transaction covered in these rules qualify as covered entities.[36] Because they provide medical services, municipal ambulance service providers are HIPAA-covered entities, but only if they transmit, in electronic form, the health information they create or receive.[37] HIPAA focuses its attention on creating uniform information in health care to improve the efficiency of transactions and to ease access for patients. The "transactions" referred to in the definition of covered entity are "transmission[s] of information between two parties to carry out financial or administrative activities related to health care."[38]

Uniform definitions of the data elements that make up these standards are critical to the viability of the standards. Implementation guides, which were provided for in the rule, set forth a Data Element Dictionary to provide uniform definitions.[39] The Data Element Dictionary includes names for each data element, definitions, and references to the transactions in which they are used.[40] Code sets are standardized data that make up the data elements.[41] Public and private organizations have developed the code sets, which have had widespread previous use in Medicare and Medicaid documentation.[42]

Prior to the promulgation of a uniform transaction and code sets rule, the health care industry conducted transactions using local code standards.[43] Exchange of information among the over 400 different formats

32. 65 Fed. Reg. 50,317–372 (Aug. 17, 2000).
33. Defined as health plans with annual receipts of $5 million or less. 45 C.F.R. § 160.103.
34. 65 Fed. Reg. at 50,368. Small health plans were given until October 16, 2003, to comply. *Id.*
35. 45 C.F.R. § 160.102.
36. *Id.*
37. *See infra* Section III.A. Local Government as Health Care Provider.
38. 45 C.F.R. § 160.103.
39. Phoenix Health Systems, *supra* note 30. The implementation guides can be downloaded from the Washington Publishing Company at http://www.wpc-edi.com. 65 Fed. Reg. 50,368; 45 C.F.R. § 162.920(a)(1).
40. Phoenix Health Systems, *supra* note 30.
41. Phoenix Health Systems, *supra* note 30.
42. Phoenix Health Systems, *supra* note 30.
43. *See* American Medical Association, *HIPAA Preparedness: What You Need to*

was inefficient because software designed to work with one standa was often incompatible with the others.[44] For example, before the TC rule, when a health care provider received the payment of a claim f a particular treatment from the insurance company, the explanation payment that accompanied it contained codes and descriptions bas on that insurance company's local codes.[45] A payment received from different insurance company for an identical treatment was often e tirely different because it was based on the second insurance company local codes.[46] The TCS rule improves efficiency by eliminating the ne to "translate" one code set to another. By improving the uniformity standards and reducing paper in these transactions, HHS expects th savings to the health care industry will be nearly $30 billion in the ne ten years.[47]

In December 2001 most covered entities were given the opportuni to extend by one year the date for compliance with the TCS rule.[48] Th extension was conditioned upon the covered entity's submission of compliance plan outlining how the entity would come into compliand before October 16, 2003.[49] Covered entities that filed for an extensic had an obligation to begin testing their system by April 16, 2003. Unaffected by this extension were small health plans, which alreac were required to comply by October 16, 2003.[51]

The Centers for Medicare and Medicaid Services (CMS), an agenc of the Department of Health and Human Services, will carry out th enforcement of the TCS rule.[52] Enforcement of the privacy rule pr marily will be triggered by complaints against covered entities.[53] Co ered entities will also have available a series of progressive steps th

Know About Transaction and Code Sets Standards, available at http://ww ama-assn.org/ama/pub/category/6776.html (last visited Feb. 8, 2003).

44. *See* Phoenix Health Systems, *supra* note 30.

45. Hypothetical based on information received in an online interview with Cynth Ransburg-Brown, Attorney, Sirote & Permutt, P.C. (Feb. 8, 2003).

46. *Id.*

47. Department of Health and Human Services, *Administrative Simplification Und HIPAA: National Standards for Transactions, Security and Privacy,* Fact Sheet (Ma 3, 2003), *available at* http://www.hhs.gov/news/press/2002pres/hipaa.html (last visit Jan. 5, 2003).

48. Administrative Simplification Compliance Act, § 2(a)(1), 42 U.S.C. § 1320d-

49. Administrative Simplification Compliance Act, § 2(a)(2), 42 U.S.C. § 1320d-

50. *See id.*

51. Department of Health and Human Services, *supra* note 47.

52. Department of Health and Human Services, *CMS Named to Enforce HIPA Transaction and Code Sets Standards,* Press Release October 15, 2002, *available* http://www.hipaacomply.com/CMS%enforces%20Code%20Sets.htm (last visited De 26, 2002).

53. *Id.*

will enable them to demonstrate their compliance or tender plans for corrective action.[54] Complaints about a covered entity's use of a non-standard code, or the non-use of a standard code where one is required, must be in writing and must be filed within 180 days of the act or omission that is the subject of the complaint.[55] Complaints may trigger an investigation, which could include a review of the covered entity's HIPAA policies, procedures, or practices, by the HHS.[56] A person who violates the TCS rule can be personally liable for penalties of up to $100 dollars per violation,[57] and identical repeat violations of the TCS rule are not capped until they reach a total of $25,000 per year.[58]

2. UNIQUE IDENTIFIERS

Under HIPAA, the Secretary of the Department of Health and Human Services must also adopt standards for creating unique identifiers for use in the health care system.[59] Covered entities will be required to utilize uniform identifiers for each employer, health care provider, health plan, and individual in the system.[60] Congress also delegated to HHS the task of developing the purposes for which these identifiers will be used.[61]

HHS issued its final rule regarding the implementation of a standard unique identifier for employers in May 2002.[62] Employer is defined by cross-referencing the Tax Code definition.[63] The Employer Identification Number (EIN) was chosen as the standard unique identifier for employers.[64] This number, which is assigned and maintained by the Internal Revenue Service, previously existed and was used by all businesses that paid wages to employees.[65] Most covered entities must comply with this standard no later than July 30, 2004.[66] With unique employer identifiers in place, there will be less chance of confusion (and therefore less chance of an improper disclosure of Protected Health

54. *Id.*

55. *See* 45 C.F.R. § 160.306(b). A description of the acts or omission that constitute the alleged violation and the name of the entity being complained against are elements of the complaint. *Id.* § 160.306(b)(2).

56. *Id.* § 160.306(b)(4)(c).

57. 42 U.S.C.A. § 1320d-5.

58. *Id.*

59. 42 U.S.C.A. § 1320d-2(b).

60. *Id.*

61. *Id.*

62. 67 Fed. Reg. 38,009–20 (May 21, 2002).

63. *See* 67 Fed. Reg. at 38,010; 45 C.F.R. § 160.103. An employer is a person for whom an individual performs or performed any service, of any nature, as the employee of that person. 26 U.S.C. § 3401(d).

64. 67 Fed. Reg. 38,009, 38,016; 45 C.F.R. § 160.605.

65. Tabatzky, *supra* note 19.

66. 45 C.F.R. § 162.600.

Information (PHI)) in instances where the exchange of health care information occurs between insurance companies and businesses with the same or similar names.

HHS published its proposed rule for a standard health care provider identifier in May 1998.[67] The national provider identifier, which is an eight position, alphanumeric identifier maintained by the Centers for Medicare and Medicaid Services, has been proposed as the standard.[68] The Health Care Financing Administration originally began to develop the national provider identifier in 1993 to foster uniformity in the Medicare and Medicaid programs.[69] When it becomes mandatory to comply with this rule, the past problem of making certain that PHI is returned to the correct "Baptist Hospital" will be eliminated because a hospital with a common name such as this will be recognized by its national provider identifier number instead. Projected publication of the final rule for the provider identifier was early spring 2003.[70]

HHS is also currently working on a proposed rule to establish standard unique identifiers for health plans.[71] The estimated publication date for this notice of proposed rulemaking is also early spring 2003.[72] Despite HIPAA's mandate, HHS currently has no plans to adopt a personal identifier for each individual in the health care system.[73] Development of this standard was put on hold indefinitely, pending the establishment of comprehensive privacy protections.[74]

3. SECURITY AND ELECTRONIC SIGNATURES

One health care industry concern arising from HIPAA's requirement of simplification and the use of electronic records is the increased potential for physical breaches of privacy related to an individual's health information.[75] Once uniform transaction components are in place and the risk of transmitting health information to the wrong entity is reduced, it is necessary to construct a system to protect against the misuse of this simplified information. After nearly four and one-half years of review, the Department of Health and Human Services finalized the security rule in February 2003 to address one aspect of this problem.[76]

According to one commentator, "[t]he single most unpredictable factor in the security of any system is physical security."[77] Security is different from both privacy and confidentiality; it is comprised of the "spectrum of physical, technical and administrative safeguards that are put in place to protect the integrity, availability and confidentiality of information."[78] Privacy addresses an individual's desire to keep certain personal information from public view, while confidentiality touches upon an entity's duty not to allow the personal information it possesses to pass to the public through an internal source. Security on the other hand, focuses on the safeguards a covered entity must put into place to keep outside sources from pulling personal information that is held within the entity into the public domain.

The security rule became effective on April 21, 2003, and covered entities will be required to comply with its provisions beginning April 21, 2005.[79] These security standards will apply to all health information either maintained or transmitted electronically by a covered entity.[80] The rule requires all covered entities to assess the potential risks and vulnerabilities to individual health data in its possession and develop, implement, and maintain appropriate security measures.[81] Requirements of the standard, which are intended to set a *minimum* level of security, include administrative procedures, physical safeguards, and technical security services and mechanisms to guard health information.[82]

Administrative procedures requirements contain eight standards including the implementation of security management procedures, workforce security measures, contingency plans for system emergencies, security awareness and training, and an evaluation process.[83] Four categories of minimum physical safeguards mandate, among other things, facility access controls, device and media controls, and the creation of

67. 63 Fed. Reg. 25,230 (May 7, 1998).
68. 63 Fed. Reg. 25,328. The national provider identifier is known as the "NPI" in the health care industry. The proposed rule notes that the Health Care Financing Administration (HCFA) maintains the NPI, however, Health and Human Services Secretary Tommy G. Thompson changed the name of HCFA to the Centers for Medicare and Medicaid Services in an announcement in June 2001. Press Release, Department of Health and Human Services, *The New Centers for Medicare and Medicaid Services (CMS),* June 14, 2001, *available at* http://www.hhs.gov/news/press/2001pres/20010614a.html (last visited Jan. 12, 2003).
69. *See* 63 Fed. Reg. 25,231.
70. Phoenix Health Systems, *Status of HIPAA Regulations Compliance Calendar, available at* http://www.hipaadvisory.com/regs/compliancecal.htm (last visited Mar. 28, 2003).
71. Department of Health and Human Services, *supra* note 47.
72. Phoenix Health Systems, *supra* note 70.
73. Department of Health and Human Services, *supra* note 47.
74. Department of Health and Human Services, *supra* note 47.
75. *See* Phoenix Health Systems, *The HIPAA Security Rule (NPRM): Overview, available at* http://www.hipaadvisory.com/regs/securityoverview.htm (last visited Dec.

76. *See* 68 Fed. Reg. 8,334 (Feb. 20, 2003). The Security Rule was originally proposed in 1998. *See* 63 Fed. Reg. 43,242 (Aug. 12, 1998).
77. Tabatzky, *supra* note 19.
78. Phoenix Health Systems, *supra* note 75.
79. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003).
80. *Id.* at 8,374 (to be codified at 45 C.F.R. § 160.103).
81. *Id.* at 8,377 (to be codified at 45 C.F.R. § 160.308).
82. *See id* at 8,377–78 (to be codified at 45 C.F.R. §§ 160.308–164.312).

secure workstations.[84] Technical security measures must include standards for access and audit controls, data and entity authentication features, and transmission security measures.[85] The rule also requires entities using network controls in its system to include alarms, audit trails, entity authentication, and event reporting.[86] Although early reports suggested the final security rule would be published before the end of 2001,[87] publication of the final rule did not occur until February 20, 2003.[88] Providers, such as municipal ambulance services, should plan to make compliance with the security rule the third phase of their HIPAA compliance program.[89]

One adverse side effect of shifting to completely electronic transactions is a reduced level of confidence that the information exchanged is authentic or that it has not been tampered with. Electronic signatures are designed to secure the authenticity and integrity of electronically exchanged documents. Without electronic signatures or other authentication devices, it is possible for anyone to infiltrate a network and access PHI.[90] As originally proposed, the security rule also contained a component consisting of standards for electronic signatures.[91] HHS proposed the use of a digital signature, which requires an entity to use a public-key infrastructure to verify the identity of the sender and that a document sent electronically has not been tampered with.[92] The proposed rule did not mandate the use of electronic signatures; these standards will apply to entities that elect to use electronic standards in health care transactions.[93] The proposed security rule also mandated that an electronic signature be created using a method that assures the document's authenticity, impenetrability, and that the sender cannot deny the fact that he or she sent it.[94] The electronic signature standard is currently on hold, however, because no consensus for an industry-wide standard could be divined from the public comments received in response to the proposed rule's publication.[95] The final security rule ultimately deleted the electronic signature section altogether, noting simply "[t]his section will be issued as a separate future regulation."[96] Electronic signature requirements will certainly be promulgated in the future because of their overarching importance to the viability of electronic transaction security. Covered entities should keep the goal of these requirements in mind as they work to comply with the security rule to avoid duplication of efforts when these regulations do resurface.

84. Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8,378 (to be codified at 45 C.F.R. § 164.310).
85. *Id.* at 8,379 (to be codified at 45 C.F.R. § 164.312).
86. *Id.*
87. *See* Phoenix Health Systems, *supra* note 75.
88. Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8,334. *See also* Phoenix Health Systems, *December 2002 News Archives: December 30, 2002 Security Rule Delayed for Fine-Tuning, available at* http://www.hipaadvisory.com/news/newsarchives/dec02.htm (last visited Jan. 4, 2003).
89. Keeping in mind that compliance with the TCS rule was mandatory in October 2002 or will be in October 2003, and that the privacy rule compliance date was April 14, 2003.
90. *See* Tabatzky, *supra* note 19.
91. *See* 63 Fed. Reg. 43,242, 43,268–69 (Aug. 12, 1998).
92. *See id.* Public-key infrastructure utilizes two lengthy prime numbers to scramble and unscramble messages sent online. *See* Mike Rothman, *Public-key Encryption for Dummies,* NETWORK WORLD FUSION, May 17, 1999, *available at* http://www.nwfusion.com/news/64452_05-17-1999.html (last visited Feb. 1, 2003). One key is a private key, which is maintained exclusively by an individual. *See id.* The other is a public key, which can be accessed by everyone else. *Id.* To assure that an individual actually signed a document, the document itself is processed through a complex mathematical formula to create a single large number called a hash. *Id.* An individual creates a hash from the document he or she wishes to transmit and then "signs" it with his or her private key. *Id.* The recipient of the document then unscrambles the document with the sender's public key to verify that the sender did in fact authenticate the document. *See* Mike Rothman, *Public-key Encryption for Dummies,* NETWORK WORLD FUSION, May 17, 1999, *available at* http://www.nwfusion.com/news/64452_05-17-1999.html

4. PRIVACY AND CONFIDENTIALITY STANDARDS

A third major area in which HHS promulgated rules is the privacy of individuals' health information. The privacy rule primarily outlines procedures to assure the availability of health information to the individual who is its subject, while prescribing standards to assure that entities will protect the confidentiality of this sensitive information. This rule reflects five principles outlined in 1997 recommendations for privacy protection by then-Secretary of Health and Human Services, Donna Shalala.[97] Those principles are consumer control of information, boundaries for use and disclosure of information, accountability for violations, public responsibility issues, and security of private health information.[98] The privacy rule was published in December 2000 but, due to a minor paperwork problem, congressional review was delayed two months.[99] As a result, the effective date for the privacy rule was

93. *See* 63 Fed. Reg. 43,242, 43,268–69 (proposed Mar. 7, 1991).
94. *See id.*
95. *See* National Committee on Vital and Health Statistics, *Annual Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act* (Nov. 12, 2002), *available at* http://www.ncvhs.hhs.gov/yr5.htm (last visited Feb. 1, 2003).
96. Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8,334, 8,367 (Feb. 20, 2003).
97. Press Release, U.S. Department of Health and Human Services, *HHS Announces Final Regulations Establishing First-Ever National Standards to Protect Patients' Personal Medical Records* (Dec. 20, 2000), *available at* http://www.hhs.gov/news/press/2000pres/20001220.html (last visited Jan. 4, 2003).
98. *Id.*

pushed back to April 14, 2001.[100] The rule had a two-year compliance window, thus covered entities were required to comply beginning April 14, 2003.[101]

The information used in the health care industry can be classified at varying levels of breadth; for that reason, several terms related to the information used in the health care system warrant explanation. The first of these is "health information." This term refers to the information that a covered entity creates or receives in the course of its business that relates to the individual's condition, the entity's provision of care, or payment for the services provided.[102] "Individually identifiable health information" is a subset of health information.[103] Individually identifiable health information, which can include demographic information about a person, is broadly defined as health information that is created or received by a covered entity and "identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[104] The privacy rule deals specifically with "protected health information" (PHI), which is individually identifiable health information that is transmitted in electronic form, maintained as electronic media, or is transmitted or maintained in any other form or medium.[105] PHI excludes, however, employment records held by a covered entity as an employer, education records covered by the Family Educational Rights and Privacy Act,[106] and records specifically described in that Act at 20 U.S.C. § 1232g(a)(4)(B)(iv).[107]

a. Application to Municipal Ambulance Service Providers

You will recall that covered entities are health plans, health care clearinghouses, or health care providers who transmit information in electronic form in connection with a transaction covered in the privacy rule.[108] A health care provider is, among other things, a provider of medical or other health services, which is further defined at 42 U.S.C. § 1395x(s).[109] Section 1395x(s) includes as medical or health services, ambulance service when the use of other methods of transportation is inappropriate considering the individual's medical condition at the time transport is necessary.[110] Considering these definitions, a local government that operates an ambulance service and transmits health information in electronic form, which is usually the case for billing purposes, is a covered entity. Ambulance services that are not currently making electronic transactions, but that do bill Medicare for their services have not totally escaped covered entity status. The same legislation that permitted the one-year extension for TCS rule compliance also requires HHS to deny payments for claims that are not submitted in electronic form beginning on October 16, 2003.[111]

b. General Rules for the Use and Disclosure of Protected Health Information

The Department of Health and Human Services promulgated a total of ten general standards regarding the use and disclosure of PHI; a sample of the subject matter follows.[112] Covered entities cannot use or disclose PHI in any ways other than those outlined in the rule.[113] HHS does, however, make allowances for incidental uses and disclosures of PHI so long as the covered entity has the proper safeguards in place and is in compliance with the minimum necessary standard.[114] Other permitted uses and disclosures of PHI include those to the individual who is the subject of the information, for the purposes of treatment, payment, or health care operations, and those made pursuant to valid authorization by the individual.[115] Covered entities are required to make disclosures of health information when requested to do so by the individual or by the Office of Civil Rights as a part of a compliance investigation.[116]

Covered entities are subject to a "minimum necessary" requirement under the privacy rule.[117] This compels covered entities to make rea-

100. Phoenix Health Systems, *supra* note 17.
101. *See* Phoenix Health Systems, *supra* note 17.
102. 45 C.F.R. § 160.103. Specifically:

> any information, whether oral or recorded in any form or medium, that:
> (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Id.
103. *Id.*
104. *Id.*
105. 45 C.F.R. § 164.103.
106. 20 U.S.C. § 1232g (2003).
107. 45 C.F.R. § 164.103.
108. *See supra* Section II.C.1.
109. 42 U.S.C. § 1320d(3).
110. 42 U.S.C. § 1395x(s).
111. Administrative Simplification Compliance Act, Pub. L. No. 107–105, 2001 U.S.C.C.A.N. (115 Stat.) 1003 (to be codified at 42 U.S.C. § 1395y).
112. 45 C.F.R. § 164.502.
113. 45 C.F.R. § 164.502(a).
114. *See* 45 C.F.R. § 164.502(a)(1)(iii).
115. 45 C.F.R. § 164.502(a)(1).
116. 45 C.F.R. § 164.502(a)(2).
117. 45 C.F.R. § 164.502(b).

sonable efforts to limit the amount of PHI used, disclosed, or requested from another covered entity, to the minimum necessary to accomplish the purpose for which the information is to be used.[118] Minimum necessary requirements do not apply to several types of transactions, including those to or from a health care provider for the purpose of medical treatment, transactions with the individual, and to the Office of Civil Rights for enforcement purposes.[119]

The general rules also set forth the standard for disclosures to a covered entity's business associates.[120] Business associates are persons who use PHI to perform functions or provide services on behalf of a covered entity.[121] Examples of these services include management, legal, financial, accounting, and consulting services provided to the covered entity.[122] Covered entities must obtain assurance from their business associates that they will properly safeguard protected health information before the covered entity can send them PHI.[123] Assurances received from business associates must be memorialized in a writing that evidences the fact that the business associate meets the requirements of the rule.[124]

c. Organizational Requirements

Seven standards for organizational requirements of covered entities are found in the rule.[125] Following is a closer look at two of those: hybrid entities and business associate contracts.

(i) *Hybrid Entities.* Covered entities are, among other things, required to conduct training for their entire workforce regarding the entity's new HIPAA policies and procedures. For a local government, this potentially would include employees, like those in the planning or public works departments, who are very unlikely to have contact with PHI. Although the vision of massive HIPAA training sessions for the entire workforce of the city or county may have sent a chill down the spines of some municipal administrators or attorneys, they can take solace in the existence of the hybrid entity provisions. Hybrid entities are individual legal entities that qualify as covered entities, but whose business

118. *Id.*
119. *See* 45 C.F.R. § 164.502(b)(2).
120. 45 C.F.R. § 164.502(e).
121. *See* 45 C.F.R. § 160.103.
122. *See id.*
123. 45 C.F.R. § 164.502(e)(1)(i).
124. 45 C.F.R. § 164.502(e)(2).
125. *See* 45 C.F.R. § 164.504.

activities consist of functions that both would and would not be subject to HIPAA if they were operating alone.[126]

For a municipality, a noncovered function would include services such as street repairs conducted by the public works department. An example of a covered function, on the other hand, might be the legal analysis done by the city attorney to determine whether the city can release accident reports to the press. Excluding, perhaps, stand-alone ambulance districts that exist in some states,[127] most municipal ambulance services are but one part of a larger local government entity. Viewing these entities in their entirety, it is evident that some components have contact with PHI at varying levels while others do not. Therein lies the beauty of the hybrid entity. Although the government unit qualifies as a covered provider, it has business activities that include both covered and noncovered functions.[128]

Hybrid entity status is not automatic for organizations that meet this definition, however.[129] The local government entity will need to designate its health care components, including the specific functions of some departments that deal with PHI, and document those designations.[130] By making these designations, a municipality can significantly reduce its compliance costs and exposure to liability by eliminating a large percentage of its employees and operations from HIPAA applicability. The privacy rule does not set forth a procedure for designation of health care components, except that an entity must designate any component of its business that would qualify as a covered entity if it were a stand-alone operation.[131] Adoption of a resolution or ordinance setting forth these designations would certainly be acceptable.

The requirements of the privacy rule only apply to the hybrid entity's health care components.[132] Hybrid entities are required to create firewalls to ensure that its health care components do not disclose PHI to other components within the operation.[133] This does not mean, however, that a hybrid entity must designate entire divisions of its business that perform only certain functions that would qualify it as either a covered entity or a business associate.[134] Instead, the rule simply permits the

126. *See id.*
127. *See, e.g.,* MO. REV. STAT. §§ 190.001–190.245 (2000).
128. *See* 45 C.F.R. § 164.504.
129. *See id.*
130. *Id.* 45 C.F.R. § 164.504 (iii)(c).
131. *Id.*
132. 45 C.F.R. § 164.105(i).
133. *See* 45 C.F.R. § 164. 105(ii)(b).
134. Rule Modification, 67 Fed. Reg. 53,182, 53,204 (Aug. 14, 2002).

covered entity to designate functions with the division that support health care activities.[135] For example, a local government agency operating an ambulance service would be allowed to designate specific functions within its legal department or finance department that support the ambulance service. It is acceptable for an employee to perform duties for both a health care component and a noncovered component provided that the employee is prohibited from disclosing PHI created or received in conjunction with his or her work for the health care component.[136]

(ii) *Business Associates.* Much like the effect of the privacy rule on covered entities, the business associate contract establishes permitted and required uses and disclosures of PHI by business associates.[137] In the context of local government, an ambulance district, for example, may contract with an outside firm to perform its billing activities. In this example the billing service would not likely qualify as a covered entity alone, but as a result of providing its services to the ambulance district, it comes into contact with PHI. The rule requires covered entities and their business associates to execute business associate contracts to establish the permitted and required uses, as well as prohibited disclosures of protected health information by the business associate.[138] In effect, business associates that otherwise would not be required to comply with HIPAA assume HIPAA compliance responsibilities through contractual obligations with a covered entity. It is possible for one covered entity to be the business associate of another covered entity.[139] Because it is impracticable for a covered entity to contract with itself, the rule does not require a hybrid entity to enter into business associate agreements between its internal health care components and noncomponents.[140] It will, however, be necessary for covered entities to modify their contractual relationships with external business associates.

Three rough categories of minimum contract provisions can be distilled from the rule: PHI protection, availability of information, and termination clauses. To protect PHI handled by business associates in the course of their services for the covered entity, the business associate must promise not to use or further disclose PHI other than that allowed

135. *Id.*
136. 45 C.F.R. § 164.504(c)(2)(iii).
137. *See* 45 C.F.R. § 164.504(e)(2).
138. 45 C.F.R. § 164.504(e).
139. *Id.*
140. Standards for Privacy and Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,203 (comments on final rule published Aug. 14, 2002).

by the terms of the agreement, to use safeguards to prevent use or disclosure to other than that allowed in the contract, to report any use or disclosure outside the contract terms to the covered entity, and to ensure that any agents, to whom the business associate provides PHI in a similar relationship will agree to the same terms.[141] Business associates must also agree to make the PHI it holds available to individuals upon request, and for amendment purposes.[142] Provisions allowing individuals to require an accounting of disclosures and inspections by the Office of Civil Rights for compliance purposes also must be contained in the business associate contract.[143]

A municipality needs to identify the relationships it has with outside entities to determine if PHI is shared. Disclosure might occur in this manner through contract billing services, legal advice, or accounting, for example. Relationships like these may trigger an obligation to modify existing contracts with these business associates.[144] Remember also that a governmental agency that qualifies as a covered entity may still be the business associate of another covered entity.[145] These relationships may require even noncovered components of a hybrid entity to take on HIPAA compliance responsibilities.[146] Examples of situations that may present business associate relationships are mutual aid agreements or the affiliation with the medical director who oversees the municipality's emergency medicine program.

HHS creates a transition period to allow covered entities and their business associates to adjust their contract documents.[147] If a covered entity executed an agreement before October 15, 2002, the provisions of that document are deemed to be in compliance with the privacy rule until the earlier of the date it is to be renewed or modified or April 14, 2004.[148]

d. Uses and Disclosures of Private Health Information

(i) *Treatment, Payment and Health Care Operations.* A covered entity generally may use or disclose PHI in carrying out its treatment, payment, or health care operations.[149] Covered entities may disclose PHI to a health care provider for its treatment activities, or to another

141. 45 C.F.R. § 164.504(e)(2)(ii).
142. *Id.*
143. *Id.*
144. *See* 45 C.F.R. § 164.504; § 164.532.
145. *See* 45 C.F.R. § 164.504(e).
146. *See* 45 C.F.R. § 164.504(e)(2)(ii).
147. *See* 45 C.F.R. § 164.532(d).
148. *See* 45 C.F.R. § 164.532(e).
149. 45 C.F.R. § 164.506(a) (PHI might be used for operation when a paramedic is receiving a performance review, or for quality assurance reasons).

covered entity or health care provider for payment purposes.[150] Provided that each entity has had a relationship with the individual whom is the subject of the PHI, the covered entity may disclose the PHI to another covered entity for health care operations purposes.[151]

(ii) *Use of Private Health Information for Which Authorization Is Required.* To use PHI for marketing purposes or to use or disclose psychotherapy notes, a covered entity must first obtain valid authorization from the individual.[152] The privacy rule sets forth core elements and required statements that establish the validity of an authorization,[153] but because these purposes would rarely arise for municipal ambulance service providers, this article will not address this topic in any further detail.

(iii) *Uses and Disclosures of Private Health Information That Require the Opportunity for the Individual to Agree or to Object.* Under the privacy rule, covered entities are required to inform an individual in advance and provide the individual an opportunity to agree or object to the use or disclosure of PHI regarding facility directories and involving others in the individual's care and for notification purposes.[154] Involving others in an ambulance patient's care and notification activities are common occurrences for ambulance service providers. When the patient is present and has the capacity to make health care decisions, the covered entity must either obtain the individual's agreement or infer from the circumstances that the patient does not object to the use or disclosure of PHI before it can involve a relative or close friend in the patient's care or notify that person of the patient's location, general condition, or death.[155] If the individual is not present (as may be true in the case of payment activities), or if it is impracticable to obtain an agreement or allow time for an objection due to an emergency situation or the patient's incapacity, the health care provider may "determine whether the disclosure is in the best interests of the individual" based upon his or her professional judgment.[156] Covered entities must respect an individual's privacy rule rights whether the individual is alive or dead.[157]

150. 45 C.F.R. § 164.506(c)(4).
151. *Id.*
152. *See* 45 C.F.R. § 164.508(a)(3).
153. For more information, see 45 C.F.R § 164.508(c).
154. *See* 45 C.F.R. § 164.510.
155. 45 C.F.R. § 164.510(b).
156. 45 C.F.R. § 164.510(b)(3).
157. *See* 45 C.F.R. § 164.502(f).

(iv) *Uses and Disclosures of Private Health Information for Which an Authorization or Opportunity to Agree or to Object Is Not Required.* HHS developed twelve standards to address situations that would allow a covered entity to use or disclose PHI without the individual's authorization or without an opportunity to agree or object.[158] Many of these standards address the principle of public responsibility by prospectively eliminating unintended adverse side effects of the privacy rule. Examples of such uses and disclosures are those for public health activities, health oversight activities, research purposes, and to avert serious threats to public health and safety.[159] Uses and disclosures required by law, as well as those regarding victims of abuse, neglect, or domestic violence, for judicial and administrative proceedings, and for law enforcement purposes are also included.[160] Many of the permitted uses in this section contain limitations on how much PHI may be disclosed, or requirements that in exchange for the information the individual seeking it must provide assurance that he or she made a good faith effort to notify the subject of the PHI or that the PHI will be protected form further disclosure.[161] Covered entities should review the provisions of section 164.512 before responding to administrative and judicial requests for PHI. An example of this might be a request for the municipality to produce general medical files to illustrate a point being made in a judicial or administrative proceeding.[162]

e. Other Requirements

Individually identifiable health information can be "cleaned" in such a way that would allow for unrestricted use of the information.[163] This process is called de-identification.[164] A covered entity can de-identify its information by removing individual identifiers that may appear in the information.[165] The eighteen identifiers set forth in the rule are:

- Names,
- All geographic subdivisions smaller than a state,
- All elements of dates (except year) for dates directly related to an individual,

158. *See* 45 C.F.R. § 164.512.
159. *See id.*
160. *See id.*
161. *See, e.g.*, 45 C.F.R. § 164.512(e).
162. *See infra* Part III.A.
163. *See* 45 C.F.R. § 164.514.
164. *Id.*
165. 45 C.F.R. § 164.514(b)(2).

- Telephone numbers,
- Fax numbers,
- Electronic mail address,
- Social Security numbers,
- Medical record numbers,
- Health plan beneficiary numbers,
- Account numbers,
- Certificate/license numbers,
- Vehicle identifiers and serial numbers, including license plate numbers,
- Device identifiers and serial numbers,
- Web Universal Resource Locators (URLs),
- Internet Protocol (IP) address numbers,
- Biometric identifiers, including finger and voice prints,
- Full face photographic images, and
- Any other unique identifying number, characteristic, or code.[166]

Provided that "the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information," information that has had its identifiers removed is de-identified.[167] It is also possible to have an expert determine that the information could be used to identify an individual.[168]

With respect to PHI, the privacy rule compels a covered entity to establish minimum necessary requirements for the use, disclosure, and request for information.[169] It is incumbent upon a covered entity to determine which employees or classes of employees in its workforce need to use PHI in their job tasks.[170] Once these individuals have been identified, the covered entity must then identify the categories of PHI those employees need and how they need to access it.[171]

Similar procedures are required for disclosures of PHI.[172] Outside of relying on criteria developed by the covered entity for determining the amount of PHI to disclose when information is requested by an outside source, covered entities may reasonably rely on statements by public officers, other covered entities, and business associates that the information they are requesting is the minimum necessary required for the purpose of the request.[173] Covered entities must also limit their requests for PHI from others in a similar fashion.[174]

166. 45 C.F.R. § 164.514(b)(2)(i).
167. 45 C.F.R. § 164.514(b)(2).
168. 45 C.F.R. § 164.514(b)(1).
169. 45 C.F.R. § 164.514(d).
170. 45 C.F.R. § 164.514(d)(2).
171. *Id.*
172. *See* 45 C.F.R. § 164.514(d)(3).

f. Notice of Privacy Practices

Individuals have a right to receive adequate notice of the uses and disclosures a covered entity might make of their PHI.[175] Individuals also have a right to adequate notice of his or her rights with respect to PHI and the covered entity's duties under the privacy rule.[176] HHS explicitly outlines the content of the notice forms that a covered entity must provide.[177] These notices of privacy practices are commonly referred to as "NPPs" among individuals who are actively pursuing HIPAA privacy rule compliance. The required elements of an NPP form are: a header with a specific notice statement, a list of uses and disclosures that the covered entity is permitted or required to make, special statements regarding specific uses and disclosures when applicable, the individual's rights, the covered entity's duties, how an individual can file a complaint, the covered entity's contact person, and the effective date of the notice.[178]

A covered entity is required to provide its NPP to any person upon request.[179] As a health care provider with direct treatment relationships, a municipal ambulance service provider must also provide its NPP to the individual no later that the date its services were rendered, except when emergency treatment is provided.[180] When providing non-emergency care, an ambulance service must make a good faith effort to obtain written acknowledgment from the individual that the individual received notice.[181] A covered entity must document its efforts to comply with the notice requirements as set forth in the rule.[182]

g. Individual's Rights Regarding Private Health Information

Individuals possess the right to request that the covered entity restrict its uses and disclosures of PHI for treatment, payment, and health care

173. 45 C.F.R. § 164.514(d)(3)(iii).
174. *See* 45 C.F.R. § 164.514(d)(4).
175. 45 C.F.R. § 164.520(a)(1).
176. *Id.*
177. *See* 45 C.F.R. § 164.520(b).
178. *Id.*
179. 45 C.F.R. § 164.520(c).
180. 45 C.F.R. § 164.520(c)(2)(i). "In an emergency treatment situation, [the covered entity should provide notice] as soon as reasonably practicable after the emergency treatment situation." *Id.*
181. 45 C.F.R. § 164.520(c)(ii).
182. 45 C.F.R. § 164.520(e).

operations purposes and its permitted disclosure for care and notification purposes.[183] The covered entity is not required to agree to these restrictions, but if it does so, it must honor the agreement as it would the other restrictions in this rule.[184] Covered entities must also permit individuals to request the receipt of communications of PHI in a confidential manner.[185] The covered entity must accommodate these reasonable requests, but may condition the grant of the request, except that it may not inquire into the basis of the request.[186]

With specific exceptions, individuals also have a right of access and to make copies of their PHI that is contained in a designated record set.[187] A designated record set is "[a] group of medical records maintained by or for a covered entity that is the medical records and billing records about individuals maintained by or for a covered health care provider . . . [u]sed, in whole or in part, by or for the covered entity to make decisions about individuals."[188] The covered entity must act on requests for access to PHI within thirty days.[189]

The rule provides grounds for written denials, some of which may be subject to review.[190] If a denial of access to PHI has occurred on reviewable grounds, the individual may seek review by a reviewing official.[191] The reviewing official is a licensed health care professional who did not take part in the original denial decision, and who the covered entity designated once the request was received.[192] HHS requires documentation of designated record sets that are available for access by individuals and information regarding whom to contact for submitting requests.[193]

Individuals also have the right to have a covered entity amend PHI about the individual.[194] Action on requests for amendment must be taken within sixty days.[195] Subject to several exceptions, individuals

183. 45 C.F.R. § 164.522(a)(1).
184. *See* 45 C.F.R § 164.522(a)(1)(b).
185. 45 C.F.R. § 164.522(b)(1).
186. *Id.*
187. 45 C.F.R. § 164.524(a)(1).
188. 45 C.F.R. § 164.501.
189. 45 C.F.R. § 164.524(b)(2)(i).
190. *See* 45 C.F.R. § 164.524 (including reviewable grounds such as a licensed health care professional's determination that access to the information would endanger the life or well-being of the individual or someone else, and nonreviewable grounds like a correctional institution's ability to deny access to medical records from the prisoners who are the subject of the information).
191. 45 C.F.R. § 164.524(a)(4).
192. *Id.*
193. 45 C.F.R. § 164.524(e).
194. 45 C.F.R.§ 164.526(a).
195. 45 C.F.R. § 164.526(b)(2).

also have a right to an accounting of the covered entity's disclosures of PHI for up to the past six years.[196] The accounting must be provided within sixty days of the individual's request and must include the date of the disclosure, the name of the individual who received the information, and a brief description of the PHI.[197] Covered entities are required to document and retain disclosures subject to the rule, as well as the actual accountings provided, and the name of the person to whom requests for an accounting should be made.[198]

h. Administrative Requirements

Covered entities are required to comply with eleven standards for administrative requirements.[199] Regarding personnel, the covered entity must designate a privacy official, whose responsibilities include development and implementation of the covered entity's privacy policies and procedures.[200] A contact person must also be designated for the purposes of providing notice and receiving complaints.[201] A covered entity was required to train all of its employees on its policies and procedures regarding PHI by April 14, 2003.[202] Once training has completed, covered entities have a continuing responsibility to train newly hired employees within a reasonable time after the beginning of their employment.[203] Covered entities are also required to train its employees within a reasonable time after a material change in its privacy rule-related policies or procedures.[204]

Apart from the forthcoming requirements of the security rule, the privacy rule requires covered entities to put into place administrative, technical, and physical safeguards to protect PHI from breaches of privacy.[205] Procedures for making complaints regarding the covered entity's policy[206] and the enforcement of sanctions against employees who violate the procedures are also required.[207] If PHI is disclosed in violation of the privacy rule, the covered entity must mitigate the harmful effects of that disclosure.[208] Providers may not condition treatment of their patients on a waiver of the individual's HIPAA privacy rights,[209]

196. 45 C.F.R. § 164.528(a)(1).
197. *See* § 164.528.
198. 45 C.F.R. § 164.528(d).
199. *See* 45 C.F.R. § 164.530.
200. 45 C.F.R. § 164.530(a)(1)(i).
201. 45 C.F.R. § 164.530(a)(1)(ii).
202. 45 C.F.R. § 164.530(b)(2).
203. *See id.*
204. 45 C.F.R. § 164.530(b)(2).
205. 45 C.F.R. § 164.530(c)(1).
206. 45 C.F.R. § 164.530(d)(1).
207. 45 C.F.R. § 164.530(e)(1).
208. 45 C.F.R. § 164.530(f).
209. 45 C.F.R. § 164.530(h).

nor may a covered entity retaliate against an individual for exercising his or her rights or for filing a complaint.[210]

Covered entities are required to implement policies and procedures designed to achieve compliance with each of the standards and implementation specifications set forth in the rule.[211] These policies and procedures should be reasonable in light of the entity's size and type.[212] A covered entity must maintain its policies and procedures, written communications, and any activity, action, or designation for which the rule requires documentation, for the period of six years from the latter of its creation or the date it was last in effect.[213]

III. Issues Confronted by Municipal Ambulance Service Suppliers

A. *Preemption of State Open Record Laws*

One issue that arises regarding the application of the privacy rule to a local government agency is how the agency should handle the tension between HIPAA's privacy requirements and state open record laws or laws that require the reporting of some medical information. The privacy rule generally preempts any contrary provision of state law.[214] For the purposes of preemption, "state law" refers to the state's "constitution, statute, regulation, common law, or other State action having the force and effect of law."[215] A state law is contrary to the privacy rule if it is "impossible to comply with both the State and federal requirements," or if it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of [HIPAA]."[216] HHS can grant exceptions to this preemption clause.[217] Preemption also will not apply in cases where the state law provides for the reporting of PHI for various public health reasons.[218] To illustrate HHS's commitment to greater access to individuals and greater protections for the privacy of individually identifiable health information, the privacy rule provides that if the state law is more stringent in its requirements than the privacy rule, the state law will apply.[219]

210. 45 C.F.R. § 164.530(g).
211. 45 C.F.R. § 164.530(i)(1).
212. *Id.*
213. 45 C.F.R. § 164.530(j).
214. 45 C.F.R. § 160.203.
215. 45 C.F.R. § 160.202.
216. *Id.*
217. *See* 45 C.F.R. § 160.203(a).
218. *See* 45 C.F.R. § 160.203(c).
219. *See* 45 C.F.R. § 160.203(b).

Illustrative of this tension is Missouri's statute limiting the public's ability to inspect or copy the records of a law enforcement agency. Missouri requires that its agencies maintain a record, which must contain the name and age of accident victims, and make that record available for inspection and copying by the public.[220] Missouri, however, limits the release of accident reports by prohibiting their release for sixty days, unless requested by an "interested party."[221] Attorneys, members of the news media, and other individuals involved in the accident are interested parties that could request to see potential protected health information in these reports.[222] Tension between Missouri's Sunshine Law and HIPAA is found on two levels. First, accident reports listing the name and age of victims are records open to the general public after sixty days in Missouri; as such, it would be impossible for a city to comply with both the state and federal requirements.[223] Second, although the Missouri statute limits exposure of these records for a time, these requirements are much less stringent than those of the privacy rule.

B. *Incidental Disclosures*

To mitigate the potentially harsh effects of strict application of privacy rule standards, there are provisions that permit incidental disclosures of PHI.[224] A common question that arises for ambulance service providers is whether the privacy rule prohibits the transmission of PHI over the radio in instances where the ambulance is informing the receiving hospital of the patient's status.[225] Two possible bases support the conclusion that this type of transaction would be permitted under the privacy rule; one that is facially clear, and another that requires a little more detail in the HIPAA analysis. First, this transaction most often occurs while the ambulance service is providing treatment to the individual. A provider is permitted to disclose PHI to another provider while carrying out treatment activities.[226] Considering this regulation, it is clear that ambulance service providers will be allowed to continue using over-the-air communications to relay information to the receiving hospital.[227]

220. *See* MO. REV. STAT. § 610.200.1 (2003).
221. MO. REV. STAT. § 610.200.2.
222. *See id.*
223. Note, however, that Missouri's Sunshine Law does have a provision that allows public bodies to close records that are "protected from disclosure by law." MO. REV. STAT. § 610.021(14) (2003).
224. *See* 45 C.F.R. § 164.502.
225. *See* PAGE, WOLFBERG & WIRTH, LLC, THE AMBULANCE SERVICE GUIDE TO HIPAA COMPLIANCE 27 (2d ed. 2002).
226. 45 C.F.R. § 164.506(c).
227. *See* PAGE, WOLFBERG & WIRTH, LLC, *supra* note 225, at 28.

While the foregoing conclusion seems elementary, it is the fact that that same radio transmission to the hospital also disclosed PHI to an unknown number of individuals who were monitoring scanners that causes a more difficult HIPAA applicability issue.[228] The potential for these incidental disclosures of PHI best illustrate the confusion that the privacy rule can produce. Resolution of incidental disclosure issues is simplified when the entity has adopted reasonable safeguards and has put into place the minimum necessary standard.[229] For now, an entity's procedures created to comply with the privacy rule, and specifically the minimum necessary requirements, will define what safeguards a covered entity has put in place. The security rule defines safeguards more concretely.[230] Addressing a frequently asked question in a recent guidance document, the Office of Civil Rights specifically stated that the privacy rule does not require structural or systems changes including "[e]ncryption of wireless or other emergency medical radio communications which can be intercepted by scanners."[231] For now it seems that the privacy rule tolerates this type of disclosure of PHI, but as technology improves it is likely that the channels of communication between ambulances and hospitals will be compelled to become more secure.

C. *Workers' Compensation Issues*

Another frequent question arising in conjunction with the privacy rule centers on its effect on workers' compensation transactions. Plans or programs that provide workers' compensation or similar insurance are not covered entities under HIPAA.[232] Covered entities are permitted to disclose PHI, without allowing the individual an opportunity to agree or object, in compliance with laws that relate to workers' compensation.[233]

Workers' compensation issues provide an excellent illustration of the type of conceptual analysis the privacy rule will require, especially for hybrid entities. When a request for PHI related to a workers' compensation claim is made, the covered local government agency should first determine how it came into contact with the PHI. If the information was obtained through the exercise of its nonhealth care components or functions (i.e., in its role as an employer), it is unlikely that the privacy rule would apply. If, on the other hand, the request is made to one of the health care components, or to a component that obtained the PHI as a result of a covered function, the privacy rule will likely be implicated. In this case, the provider is permitted to disclose the PHI, in accordance with state workers' compensation laws, but only to the minimum extent necessary for the person requesting the information to complete their task.[234] Recall that the covered entity may rely on the statements by public officers or other covered entities that the information they are requesting is the minimum necessary,[235] but also keep in mind that workers' compensation programs or plans are not covered entities, so it is the ambulance service's responsibility to have developed criteria for limiting the disclosure of the PHI to the minimum amount necessary.[236] Minimum necessary determinations are not required, however, when state law requires the disclosures.[237]

228. *See id.*
229. *See* OFFICE OF CIVIL RIGHTS, OCR GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE 11 (Dec. 11, 2002), *available at* http://www.hhs.gov/ocr/hipaa/privacy.html (last visited Dec. 30, 2002). Incidental disclosures of PHI are permitted if reasonable safeguards and the minimum necessary standard had been adopted. 45 C.F.R. § 164.502(a)(1)(iii).
230. *See* 68 Fed. Reg. 8,334 (Feb. 20, 2003).
231. OFFICE OF CIVIL RIGHTS, *supra* note 229, at 15.
232. *See* 45 C.F.R. § 160.103. Workers' compensation appears on the list of excepted benefits that is referred to under the definition of "health plan." 42 U.S.C. § 300gg-91(c)(1)(D)(2003).
233. *See* 45 C.F.R. § 164.512(l).

IV. Becoming Privacy Rule Compliant

A. *Appointing Compliance Personnel*

An ambulance service provider that needs to ensure its compliance with the privacy rule can look initially to the list of administrative requirements provided at 45 C.F.R. § 164.530. The first priority should be to designate a privacy official. This official will spearhead the compliance process and will be "responsible for the development and implementation of the policies and procedures of the entity."[238] The larger the organization is, the more important it is to get a senior member of management on board to aid in entity-wide compliance.[239] Also depending upon the size of the entity, it may be necessary to form a HIPAA compliance team or committee to carry out the vast number of requirements. The municipality should consider appointing individuals from the areas of the organization that will likely be health care com-

234. *See id.*
235. *See* 45 C.F.R. § 164.514(d)(3).
236. *See* 45 C.F.R. § 164.514(d).
237. *See* 45 C.F.R. § 164.502(b).
238. 45 C.F.R. § 164.530(a)(1).
239. *See* Phoenix Health Systems, *Steps for Providers: HIPAA Gap Assessment/Risk Analysis, available at* http://www.hipaadvisory.com/action/compliance/gapassessment.htm (last visited Jan. 20, 2003).

ponents or would carry out covered functions. The ambulance service, fire department, administration, legal, information technology, and finance departments would provide the best candidates.

B. *Gap Analysis*

Once the personnel responsible for making the organization compliant have been put into place, their first priority should be an evaluation of the entire operation to consider how PHI enters and leaves, and to determine who comes into contact with it. This assessment is commonly referred to as a "gap analysis," which has the purpose of identifying gaps in the organization's current privacy policies.[240]

While conducting the gap analysis the compliance committee should take a detailed account of exactly how PHI is used in the operation, and who uses it. This information will be used to identify the local government agency's health care components and the covered functions that other departments perform for or on behalf of the health care components. It is important to be creative and keep an open mind while performing this assignment so that no element is left out of the program. Relationships among legal, finance, and administration may have been obvious, but also check the possibility that the police department may perform some covered functions. A nurse's station in the jail or at other locations would likely qualify as a covered health care component as well. The health care components and covered functions that turn up in the gap analysis need to be designated and documented according to 45 C.F.R. § 164.504(c)(3)(iii).

Municipalities should also account for outside relationships connected with the exchange of PHI. The agency should determine whether it receives PHI from an outside source to perform a service for that source. The covered entity should also check to see how PHI leaves the organization. In smaller agencies, services such as billing or legal advice may be delegated out on a contract basis. Conducting this type of assessment will aid the municipality in identifying its business associate relationships. Contracts with these entities will need to be modified to meet the privacy rule standards by at the latest April 14, 2004, but earlier in many cases.[241]

The gap analysis also enables the local government agency to address

240. *See, e.g.*, PAGE, WOLFBERG & WIRTH, LLC, *supra* note 225, at 45; Phoenix Health Systems, *HIPA Assessment: Where Are Our Vulnerabilities . . . What Are Our Risks?, available at* http://www.hipaadvisory.com/action/HIPAAssessment.htm (last visited Jan. 20, 2003).

241. *See* 45 C.F.R. § 164.532(c).

how PHI is used and what the minimum amount is that is necessary to complete a particular task. The privacy rule specifically outlines how a covered entity can use PHI.[242] Using information from this analysis, the municipality can identify which uses of PHI are for treatment, payment, or health care operations, and which other uses may require the individual's authorization or agreement before the covered entity is able to use or disclose it. At this time the characteristics of the information that cause it to be PHI can also be accounted for so that the covered entity is able to de-identify the information in accordance with 45 C.F.R. § 164.514(b)(2) if necessary. Finally, the covered entity should identify the designated record sets that PHI exists in so that individuals who request their PHI can do so more easily.

C. *Drafting Policies, Procedures, and Forms*

Once a complete inventory of PHI practices for the municipality is completed, the next step is to draft policies, procedures, and forms that serve as the infrastructure of the compliance plan. To do this the agency should individually address each of the privacy rights enumerated in the rule. These include the request for restriction of uses and disclosures,[243] requests for confidential communication,[244] the provision or denial of the right to access PHI,[245] amendments to PHI,[246] and accountings.[247]

Turning its attention inward for a moment, the covered entity should also draft its internal procedures for training, safeguards of PHI, and sanctions for employees who violate the policy.[248] Internal policies that must be developed at this time are the municipality's duty to mitigate the harmful effects of disclosures that result from a violation of the privacy rule and the covered entity's policy not to retaliate against or intimidate individuals who attempt to exercise their privacy rights.[249] A covered entity should also draft its procedures for documentation and complaints. Work on the complaint procedure should include a final personnel designation—the contact person who is responsible for receiving complaints.[250]

The covered entity's notice of privacy practice will serve as a sum-

242. 45 C.F.R. § 164.502.
243. *See* 45 C.F.R. § 164.522(a).
244. *See* 45 C.F.R. § 164.522(b).
245. *See* 45 C.F.R. § 164.524.
246. *See* 45 C.F.R. § 164.526.
247. *See* 45 C.F.R. § 164.528.
248. *See* 45 C.F.R. § 164.530.
249. *See id.*
250. *See* 45 C.F.R. § 164.530(a).

mary of the entity's privacy compliance program, and as such is best saved for last in the drafting process. Because any person has a right to receive notice of the uses and disclosures the covered entity might make with their PHI,[251] the notice of privacy practice is among the most important documents for a covered entity. As you may recall, HHS mandates the content for most of this document,[252] but the information gathered in the gap analysis is needed to fill in the details. The notice of privacy practice also provides an individual with a summary of the procedures that are available for exercising his or her privacy rights such as the requests for amendment, accounting, or the complaint procedure.[253]

D. *Training*

When all of the policies and procedures have been established, the covered entity must train all of the members of its workforce.[254] For hybrid entities, this training will need to include all employees who work in the health care components and those who perform covered functions. This training will need to cover all of the policies and procedures that comprise the municipality's compliance program.[255] The training must have been completed by April 14, 2003, and there is a continuing responsibility to train each person who comes into a position in the health care component or covered function within a reasonable time.[256] Training records need to be documented according to the covered entity's procedure and the privacy rule.[257]

E. *Maintenance of Privacy Policies and Procedures*

Training is not the only continuing responsibility of covered entities. After the compliance date passes a covered entity must continue to monitor the privacy rule and make modifications to its policies and procedures, as changes in the law require.[258] A covered entity must also retain documentation of its privacy rule related information for six years after the event that caused it, or its effective date, whichever is later.[259] Finally, a covered entity must monitor its workforce for violations of its policies and levy sanctions upon those who failed to comply.[260]

251. *See* 45 C.F.R. § 164.520.
252. *See* 45 C.F.R. § 164.520(b).
253. *See id.*
254. *See* 45 C.F.R. § 164.530(b)(1).
255. *See id.*
256. *See id.*
257. *See id.*
258. *See* 45 C.F.R. § 164.530(i)(2)(i).
259. *See* 45 C.F.R. § 164.530(j)(2).
260. 45 C.F.R. § 164.503(e)(1).

V. Enforcement

The consequences for violating HIPAA and its privacy rule are fairly steep. Civil monetary penalties for failure to comply are levied against the individual who commits the violation in the amount of up to $100 per violation.[261] Civil penalties are capped at $25,000 for "all violations of an identical requirement or prohibition during a calendar year."[262] Individuals who did not know, and could not have known, that they violated the Act will not be fined.[263]

Criminal penalties also apply to HIPAA violations where a person "knowingly and in violation of [HIPAA] . . . obtains individually identifiable health information relating to an individual; or discloses individually identifiable health information to another person."[264] General penalties for HIPAA violations can be as high as $50,000 and/or one year imprisonment.[265] The penalty increases for offenses committed under false pretenses and for violations committed with the intent to utilize the individually identifiable health information for a personal gain, with the maximum penalty reaching a $250,000 and/or ten years imprisonment.[266]

The Office of Civil Rights, an agency within the HHS, will enforce the privacy rule.[267] Office of Civil Rights expects covered entities to cooperate with them in reaching compliance, and offers technical assistance as an inducement of voluntary compliance.[268] Considering the underlying tone of HIPAA and its regulations, the following statement should make an impression: "Although enforcement by HHS' Office of Civil Rights and the Centers for Medicare and Medicaid Services will be primarily complaint-driven, and although patients or others will have to say 'ouch' to the Feds before you see uniforms at your door, some will say 'ouch'. This is the millennium of the educated consumer; fines and penalties will be exacted."[269]

Individuals who think that a covered entity is not complying with the privacy rule have the right to file a complaint.[270] Complaints must

261. *See* 42 U.S.C. § 1320d-5.
262. *Id.* (emphasis added).
263. 42 U.S.C. § 1320d-5(b)(2).
264. 42 U.S.C. § 1320d-6(a).
265. 42 U.S.C. § 1320d-6(b)(1).
266. 42 U.S.C. § 1320d-6(b).
267. Department of Health and Human Services, *supra* note 97.
268. *See* 45 C.F.R. § 160.304.
269. D'Arcy Gurin Gue & Tom Grove, *11th Hour HIPAA: How Can You Meet the Deadlines?, available at* http://www.healthmgttech.com/archives/h0103deadline.htm (last visited Jan. 20, 2003) (emphasis added).
270. *See* 45 C.F.R. § 160.306.

be filed within 180 days from the time the individual knew of the reason for the complaint.[271] On the complaint, individuals must state the name of the party involved and must describe the acts or omissions that he or she believes is a violation.[272] Complaints must be in writing, but may be in either paper or electronic form.[273] The Office of Civil Rights may commence an investigation in conjunction with a complaint that may entail a review of the covered entity's policies, procedures, and privacy practices.[274] Covered entities are required to provide records and compliance reports at the Office of Civil Rights' request, and must cooperate with all complaint investigations and compliance reviews conducted by the Office of Civil Rights.[275] If the Office of Civil Rights finds it necessary to conduct a complaint investigation or compliance review, the covered entity must permit the Office of Civil Rights to access its records during normal business hours.[276] If exigent circumstances exist, however, the Office of Civil Rights may compel the covered entity to provide access to its records at any time.[277]

VI. Conclusion

HIPAA is unquestionably a monumental piece of legislation, especially in the area of patient's privacy rights. As expansive as HIPAA is, it cannot protect all private health information from disclosure by all sources; this legislation does, however, affect the most prevalent users of private health information, and thus, makes substantial gains in the long-term goal of protecting this sensitive material. HIPAA's reach will likely extend to local governments, and most definitely to those operating municipal ambulance services. In addition to the discussion in this article, a local government agency should also be aware that it might qualify as a HIPAA-covered health plan through various insurance programs that it operates or in which it participates. For this reason, local government agencies should acquire a general familiarity with all of HIPAA's provisions and how it could apply to their specific situations.

Fortunately, there is a plethora of sources of assistance available including the advice of specialized outside counsel and HIPAA consultants, or self-help methods available through internet websites, such as the one operated by the Department of Health and Human Services. HIPAA will cause municipal ambulance service providers to modify their business practices in many ways. Local government agencies should make certain that they have taken appropriate steps to assure HIPAA compliance to avoid the consequences of enforcement by the Office of Civil Rights. Compliments go to those entities that have taken action to become HIPAA compliant; and for those that have not, remember: "According to an old Chinese proverb, the best time to plant a tree was 20 years ago (or at least one year ago, in HIPAA time). According to the same proverb, the second-best time is now."[278]

271. 45 C.F.R § 160.306(b)(3).
272. 45 C.F.R § 160.306(b)(2).
273. 45 C.F.R § 160.306(b)(1).
274. 45 C.F.R § 160.306(c).
275. 45 C.F.R § 160.310(a).
276. 45 C.F.R § 160.310(c)(1).
277. *Id.*

278. Gurin Gue & Grove, *supra* note 269.