TABLE OF CONTENTS

I. INTRODUCTION 2

II. COVERAGE OF MUNICIPAL ACTIVITIES AS HEALTH CARE PROVIDERS 2

a. Are You a Covered Entity?. 3

b. How Can You Become a Hybrid Entity? 5

c. What Is Protected Health Information? 6

III. RELEASE OF PROTECTED HEALTH INFORMATION. 6

a. Treatment, Payment, & Operations 7

b. Judicial and Administrative Proceedings 8

c. As Required by Law 8

d. Law Enforcement 9

e. Public Health Purposes

i. Public Health Activities 10

ii. Averting Serious Threats to Health or Safety . . 11

iii. Research 12

f. Other Relevant Provisions

i. Employment-Related Issues 12

ii. Business Associate Issues 13

iii. Interaction with State Law 13

IV. MINIMUM NECESSARY STANDARD 13

V. CONCLUSION 14

I. INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-91) and its attendant regulations generally protect medical information maintained by covered entities (the Privacy Rule); provide security measures for the storage of data on electronic systems (the Security Rule); and require standardization of electronic transactions of health care information (the Transaction and Code Sets Rule). The purpose of HIPAA's Privacy Rule is to more carefully guard information that health care plans and providers maintain on patients.[1]

Earlier this year, IMLA provided information at its mid-year seminar that generally explained the applicability of HIPAA's Privacy Rule to municipalities.[2] That paper discusses the applicability of HIPAA's Privacy Rule to health care providers and certain health care plans, with an emphasis on the Privacy Rule's requirements for covered entities. When necessary, this paper will reiterate some of the definitions and concepts contained in the April 2003 presentation. This paper focuses on the applicability of HIPAA to municipalities as health care providers, and discusses issues related to the release of protected health information (PHI).[3]

II. COVERAGE OF MUNICIPAL ACTIVITIES AS HEALTH CARE PROVIDERS

The Privacy Rule generally prohibits *covered entities* from using or disclosing *PHI*, *except* as permitted (or required) in the rule itself.[4] If you are a covered entity, you must have specific policies in place regarding HIPAA implementation, designate a privacy officer, train all personnel who handle PHI on the policies, maintain an inventory of released PHI, and follow other numerous requirements.[5]

---

[1] HIPAA's Privacy Rule is codified at 64 CFR Parts 160 and 164.

[2] *See* O'Brien, Andrea, What Every Municipality should know about HIPAA'S Medical Privacy Rules (April 28, 2003).

[3] The purpose of this paper is to provide general information regarding HIPAA and refer the reader to the applicable HIPAA regulations and other legal resources that discuss HIPAA implementation. It does not constitute legal advice and should not be relied upon as legal advice. The author wishes to thank Nancy Kelly, Shirley Tomasello and Linda Bosu, Assistant Directors of Law, City of Cleveland Department of Law, for their efforts in researching HIPAA issues and providing training to City of Cleveland personnel.

[4] 45 CFR §164.502.

[5] Ms. O'Brien's paper, presented in April at IMLA's mid-year conference, discusses compliance requirements for covered entities. It provides a checklist for the policies and procedures that each covered entity, or the HIPAA-covered activities of a hybrid entity, must write and follow to ensure HIPAA compliance. Please refer to that paper for HIPAA compliance assistance.

In order to determine HIPAA coverage, you must first establish if your activities categorize you as a covered entity. Then, you should understand what type of information constitutes PHI. Finally, you should have a basic understanding of how PHI can be released, which is either pursuant to an authorization of release signed by the person whose information is at issue, or through one of the myriad of exceptions specifically authorized in the Privacy Rule.

a. Are You a Covered Entity?

As explained in the April IMLA mid-year seminar HIPAA paper, HIPAA applies to health plans of a certain size, health care clearinghouses, and health care providers who transmit health care information in electronic form in connection with standardized transactions.[6] Since the April paper provides detailed discussion on what health care plans are covered, this analysis will focus on municipalities as health care providers.

The Medicare definitions of "providers of service" (institutional providers, such as hospitals) and "providers of medical or health services" (non-institutional providers, such as physicians, dentists and other practitioners) dictate whether or not you are a health care provider.[7] The Privacy Rule covers only health care providers that transmit PHI electronically in connection with a standardized transaction.

What electronic transmissions by providers trigger HIPAA privacy rule coverage? The information must be health care related, and must be sent to carry out a financial or administrative activity.[8] Just using e-mail, for example, will not automatically make you subject to the rule. Likewise, faxing a question about a patient or sending a disk with medical information to another doctor would probably not be covered.[9] Rather, the transmissions must be related to financial or administrative activities that are addressed by the Transaction and Code Sets Rule (i.e., that are "standardized" transactions) and must contain PHI.[10] Examples of transactions that would make health care providers subject to the Privacy Rule include the transmission of information related to health care

---

[6] 45 CFR §160.102.

[7] *See* 45 CFR §160.103; *see also* Summary of the HIPAA Privacy Rule, United States Department of Health & Human Services, Office for Civil Rights (Revised May 2003)(OCR Privacy Brief). Note that the Rule covers all health care providers, regardless of size, unlike the health plan provider definition.

[8] *See* 45 CFR §160.103; *see also* Lawson, Nancy A., Jennifer M. Orr and Doedy Sheehan Klar, The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements, 70 Def. Couns. J. 127, 130 (January 2003).

[9] Lawson et al., *supra* at p.130.

[10] OCR Privacy Brief at p.2. Note that the health care provider is covered whether it electronically transmits the transactions directly or uses a third party (such as a billing service) to do so on its behalf. *Id.*

claims; health care payments; the first report of injury; and referral authorizations.

As an example, the City of Cleveland, Ohio, assessed its health care provider activities to determine if it is a covered entity under HIPAA. The City determined that the following Departments (or divisions/offices within those departments) are covered entities:[11]

- Department of Public Health
  - ✓ Childhood Lead Poisoning Program
  - ✓ Health Centers (Healthcare Clinic Services)
  - ✓ Office of Mental Health & Substance Abuse
  - ✓ District Nursing Office
  - ✓ Division of Correction (Inmate Infirmary)[12]
- Department of Finance
  - ✓ Division of Licenses & Assessments (Medical Billing Services)
- Department of Personnel & Human Resources
  - ✓ On-Site Nursing Services
  - ✓ Fully-Funded Employee Health Care Plan
- Department of Public Safety
  - ✓ Division of Police
    - City Jail Nursing Services for Prisoners[13]
    - Medical Billing Services
  - ✓ Division of EMS
  - ✓ Division of Fire (EMS Services)
- Department of Port Control (Airport)
  - ✓ Division of Fire
    - EMS
    - Medical Billing Services

As you can see, providing health care at clinics, jails, and in ambulatory situations encompasses most of the health care provider services in the example above. Those medical services, along with the billing and administrative functions of the services, constitute covered activities.

---

[11] This list includes coverage as a health care plan provider. Assistant Director of Law Nancy Kelly sent questionnaires to all of the potentially affected Departments/Divisions/Offices, asking the kind of services provided; the type of information kept; the method of transmission of the information; the method of storage of the documents; etc. She then personally visited all of the offices to interview personnel and assess whether they were a covered entity – i.e., whether they were a health care provider who electronically transmitted health care information covered under the standardization rule. At that time, she also advised each covered entity of the requirement to name a privacy officer, and added the office to the list of covered entities that Law Department personnel would train before the April deadline.

[12] Note that there are special provisions regarding prisoner rights. *See* 45 CFR §164.513(k)(5).

[13] *Id.*

At this point, you may be asking how a single legal entity such as a municipality or a university manages HIPAA compliance when only certain functions of that entity are covered by HIPAA. When some services of an entity are covered, and others are not, the entity may become a "hybrid" entity and be responsible for HIPAA compliance only in those areas of covered activities.

b. How Can You Become a Hybrid Entity?

HIPAA provides a formal designation process that confers "hybrid entity" status upon entities that have both covered and non-covered functions. The term "hybrid entity" is defined as follows:

> A single legal entity:
>
> (1) That is a covered entity;
> (2) Whose business activities include both covered and non-covered functions; and
> (3) That designates health care components in accordance with paragraph ©(3)(iii) of this section.[14]

Basically, hybrid entities are required to formally designate any "component", i.e. office, division, etc., that would meet the definition of covered entity if it were a separate legal entity. This designation is then maintained with the other HIPAA policies and procedures.[15]

What is the effect of the hybrid definition? Policies and procedures can be more specific to the covered activities in a hybrid entity. For example, each covered entity must have a privacy officer and contact person. Each covered entity must maintain a log of PHI that was released. Each covered entity must have a complaint process in place to process complaints regarding HIPAA compliance. It is easier to maintain and enforce these policies, and to identify and train personnel who have access to PHI, on a limited basis based on covered activity rather than on a citywide basis.

One effect of hybrid designation, though, is that each covered component is treated as if it were its own entity for the purpose of maintaining and releasing PHI. Thus, one covered component in the city, such as the Health Department, cannot release information to anyone, including covered OR non-covered city components, unless such release is authorized under HIPAA.[16]

---

[14] 45 CFR §164.504.

[15] For an excellent discussion of the ramifications of hybrid status in the research arena, *see generally* Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule at p.6 (NIH Publication Number 03-5388).

[16] 45 CFR §164.504(c)(2).

c. What Is Protected Health Information?

The Privacy Rule protects PHI, which is all "individually identifiable health information" held or transmitted by a covered entity in any form.[17] This information includes: past, present or future health conditions; the provision of health care; and payment for any past, present or future health care. In addition, any information that can reasonably lead to an individual's identity is prohibited from being released.[18] Information that could lead to a person's identity includes social security numbers, addresses and phone numbers. In order to de-identify information and have unrestricted use of that information, you either must use a qualified statistician for the task, or remove approximately 18 pieces of information from the document regarding the individual, the individual's relatives, household members, and the individual's employer.[19]

Note that some state public records laws already prohibit cities from releasing an individual's medical information to the public.[20] What HIPAA adds, however, is the prohibition of releasing any identifying information, such as the name and address of that individual.

The remainder of this paper focuses on the day-to-day activities of municipalities, and how those activities may be affected by the HIPAA privacy regulations. It provides a more detailed analysis of when and how PHI may be released. It then provides information regarding the "minimum necessary" standard, which governs the quantity and type of PHI that may be used, released or requested by a covered entity.

III. RELEASE OF PROTECTED HEALTH INFORMATION

Cities routinely receive public records requests for information. Likewise, subpoenas may be issued to produce certain documents. In addition, one department or division of a city may request documents from another department or division.

In each of these instances, any covered entity, or covered component if it is a hybrid entity, must determine whether the document contains PHI before releasing it. If the document contains PHI, then the covered entity must determine whether the individual whose records are being sought has signed an authorization form, or whether the release of the information is otherwise

---

[17] 45 CFR §160.103; *see also* OCR Privacy Brief, *supra* n.6 at pp. 3-4.
[18] 45 CFR §160.103.
[19] 45 CFR §164.514(a) and (b).
[20] *See, e.g.,* Ohio Revised Code §149.43.

authorized under HIPAA.[21] Under what circumstances may PHI be released without authorization from the individual? There are many situations that allow the release of PHI. Discussed below are a few of these situations that affect the day-to-day operation of municipal entities. You must read the HIPAA Privacy Rule and the Department of Health and Human Services' guidance documents to understand each of the exceptions.

a. Treatment, Payment, & Operations

A covered entity may release information without an authorization for the purposes of treatment, payment, or health care operations.[22] If your city-owned clinic must obtain a second opinion from another physician regarding treatment options, must provide information to a billing service to obtain payment, or must use the information for operational purposes, an authorization is not necessary to release PHI.

Treatment and payment are fairly straightforward concepts. "Health care operations," however, is a more nebulous concept. It includes the following activities *if they relate to the covered functions of the provider*: quality assessment activities, competency assessments (such as those for accreditation), medical reviews, fraud investigations, insurance purposes, business planning, and legal services.[23]

Note that the service must be related to the covered function in order to fall under the operation definition. For instance, if legal services were necessary to defend a malpractice action at a city clinic, then any clinic record relevant to the lawsuit, including PHI, would be available to the city's legal counsel for that purpose. If those records were needed by a city attorney, but not in furtherance of the clinic's purposes (such as in an employment action in which medical condition is an issue), then you may not rely on this exception to allow disclosure without an authorization. In that situation, you would either have to obtain authorization or obtain the records through another permitted disclosure, such as through a court order.

---

[21] There are instances where an authorization is necessary, such as for the release of psychotherapy notes (except that necessary for certain specified treatment, payment or health care operations), and for the release of records for marketing purposes (with two specific exceptions). *See* 45 CFR §164.512. In addition, under certain circumstances, an individual must be given the opportunity to object to the use of the information, such as for hospital directories or communications with relatives in non-emergency situations. *See* 45 CFR §164.510.

[22] 45 CFR §164.506.

[23] The preamble to the Final Privacy Rule provides a helpful discussion of what constitutes health care operations. *See* 65 Fed. Reg. 82462, 82489 – 91 (December 8, 2000).

b. Judicial and Administrative Proceedings

When legal proceedings are not covered under the health care operations exception, records may be disclosed if you jump through several hoops. These hoops include a court or administrative tribunal order, or subpoenas and discovery requests that also include other assurances.[24]

When receiving a court or administrative tribunal order, PHI may be released. However, you may only release the information that is expressly referenced in the order.[25]

When receiving (or issuing) a subpoena or other discovery request, the requesting party must take additional steps before PHI may be released. The requesting party must demonstrate that efforts were made to notify the individual whose records are being sought of the subpoena. Upon receiving notice, the individual may object to the release of the records. In the alternative to demonstrating notice to the individual whose records are at issue, the requesting party may demonstrate that efforts were made to obtain a protective order limiting the use of the information and requiring that all copies of the information be returned upon completion of the legal matter.[26]

c. As Required by Law

PHI may also be released without an authorization when required by law. In response to comments, a definition was added to the final Privacy Rule for the phrase "required by law." This phrase is defined to mean a mandate contained in law that compels a covered entity to use or disclose PHI *and* that is enforceable in a court of law.[27] This exception specifically provides that you may only release that information required to be released and nothing more.

In the municipal setting, one example where the release of PHI might fall under state law is the reporting of EMS information to a state statistical database. In the billing arena, many Medicaid regulations require similar reporting wherein the release of PHI would be permitted if done in strict accordance with the reporting law. Note that "required by law" does not include contractual obligations wherein one party voluntarily entered into the contract and the release of PHI becomes an issue when fulfilling contractual obligations.[28]

---

[24] *See* 45 CFR §164.512(e).
[25] 45 CFR §164.512(e)(1)(i).
[26] 45 CFR §164.512(e)(1)(ii).
[27] 45 CFR §160.501; *see also* 65 Fed. Reg. 82462, 82497 (December 8, 2000).
[28] *Id.*

A specific exception under HIPAA that is related to the "required by law" exception is that for reporting suspected adult victims of domestic abuse, neglect or domestic violence.[29] Many state laws require such reporting to public health agencies, adult protective services, social service agencies, or other authorities. Note that the rule only addresses the PHI of individuals who are the suspected victim, and not other individuals such as suspects in the matter.

This exception offers three avenues to report suspected adult abuse: with the permission of the individual who is the suspected victim; specifically in compliance with any mandatory reporting requirements under state law; or in compliance with any authorized reporting requirements under state law, under certain circumstances.[30] Each of the reports must be accompanied by a notice to the individual whose information is being disclosed, except in situations where such disclosure could lead to further damage to the individual or where the notice would go to a personal representative of the individual (such as a guardian) and the covered entity reasonably believes that the representative is responsible for the abuse.[31]

d. Law Enforcement

Covered entities have specific permission to disclose PHI when state or federal law mandates such disclosure, such as those requiring the reporting of gun shot wounds.[32] In addition, when there is a suspected crime (other than abuse or neglect), law enforcement officials may obtain PHI about the suspect or the victim under certain limited circumstances.

First, when medical care is provided by EMS, or in other emergency situations off-site of the health care provider's premises, PHI may be released by the responding care provider to law enforcement personnel in order to report the commission or nature of a crime, the location of the crime or the victim(s), and the identity, description or location of a perpetrator of the crime.[33] This exception recognizes the unique role of first responders in medical emergencies. Early arrival at the scene may alert these covered entities that a crime has been committed before the apparent victim is able to communicate to the police officers. In addition, immediate reporting of the crime may increase the potential for apprehending the perpetrator.[34]

---

[29] *See* 45 CFR §164.512(c). Note that child abuse reporting is regulated under paragraph (b), which addresses disclosures for public health activities. *See* 65 Fed. Reg. 82462, 82525 – 28 (December 8, 2000).
[30] *See* 65 Fed. Reg. 82462, 82527.
[31] *Id.* at 82528.
[32] 45 CFR §512(f)(1)(i).
[33] 45 CFR §164.512(f).
[34] *See* 65 Fed. Reg. at 82533 – 34 for an educational discussion about reporting crimes in emergency situations and the interplay of state law and non-emergency situations.

Health care providers also may release PHI to law enforcement officials based upon the reasonable belief that a crime has been committed on their premises.[35] Likewise, PHI may be released to law enforcement personnel upon request for the purposes of identifying or locating a *suspect*, *fugitive*, *material witness* or *missing person*. Such release for this purpose is limited, however, to name, address, birth information, social security number, blood type, type of injury, date of treatment and a description of distinguishing physical traits.[36]

Similarly, limited PHI information may be released about the *victim* of a crime (other than in abuse/neglect cases, and other than those situations where a public health activity is implicated, in which case the particular provisions regarding those circumstances govern.) Before releasing the PHI, the provider must have the permission of the victim. If the victim is incapacitated, the provider may only release PHI if the law enforcement official represents that the information is necessary to determine if a crime has been committed and the information will not be used against the victim, that the investigation would be materially and substantially hampered by waiting to obtain the information, and, in the covered entity's best professional judgment, disclosure is in the best interests of the individual/victim.[37]

The provisions regarding law enforcement in general will have an impact on all municipalities. It is imperative that you review the law enforcement provisions in the privacy rule in their entirety, along with those provisions regarding abuse/neglect, public health emergencies, and judicial proceedings, in order to advise your police departments on their rights, and your covered components on their responsibilities.

e. Public Health Purposes

i. Public Health Activities[38]

HIPAA authorizes the disclosure of PHI without authorization for certain public health activities.[39] Public health authorities may collect or receive PHI *as authorized by law* for the purpose of preventing or controlling disease, injury, or

---

[35] 45 CFR §164.512(f)(5).
[36] 45 CFR §164.512(f)(2).
[37] 45 CFR §164.512(f)(3).
[38] Note that health oversight activities are regulated separately under 45 CFR §164.512(d) and are not discussed in this paper.
[39] *See generally* HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services, Morbidity and Mortality Weekly Report, Vol. 52 (April 11, 2003)(discussing HIPAA's impact on public health and research endeavors); and Bruce, Julie, Bioterrorism Meets Privacy: An Analysis of the Model State Emergency Health Powers Act and the HIPAA Privacy Rule, 12 Annals Health L. 75, 94 – 99 (2003)(discussing HIPAA in the context of health and safety issues).

disability.[40] These reports may include disease reporting, vital statistics (birth or death), and public health surveillance, investigations or interventions. Likewise, public health authorities and other authorities authorized by law to receive reports of child abuse or neglect are specifically covered by this exception.

PHI may also be released, *as authorized by law,* to an individual if that individual is at risk of contracting or spreading a disease or condition if the release of the information is necessary to conduct a public health investigation or intervention.[41]

Thus, a review of state and federal law reporting and notification requirements is necessary to ascertain whether HIPAA allows release of PHI for public health activities.

ii. Averting Serious Threats to Health or Safety

HIPAA allows the release of PHI (consistent with ethical and legal standards) if there is a good faith belief that such release is necessary, to avert a serious threat to the health and safety of an individual or the public.[42] The good faith belief must be based on actual knowledge or in reliance on a credible source that has apparent knowledge or authority. There is a presumption of good faith if the disclosure is made to avert a public health emergency.[43]

The Privacy Rule limits the recipient of the information to those entities that may prevent or lessen the threat, including the target of the threat, or to law enforcement officials under certain circumstances. This provision of HIPAA is consistent with the "duty to warn" doctrine that was originally adopted in California and then migrated to other states through statute or case law, although HIPAA only authorizes the disclosure and does not mandate it.[44]

PHI may be released to law enforcement officials under this exception in two limited circumstances. First, the information may be released if necessary to identify or apprehend an individual who admitted that he or she participated in a violent crime that the covered entity reasonably believes may have caused serious harm to the victim (excluding statements made in therapy or counseling

---

[40] 45 CFR §164.512(b).
[41] *Id.*
[42] 45 CFR §164.512(j).
[43] 45 CFR §164.512(j)(4); *see also* Bruce, Julie, Bioterrorism Meets Privacy: An Analysis of the Model State Emergency Health Powers Act and the HIPAA Privacy Rule, 12 Annals Health L. 75, 98 (2003).
[44] *See* 65 Fed. Reg. 82462, 82538 for a comparison between the "duty to warn" doctrine and the Privacy Rule.

sessions). Second, the information may be released if the circumstances indicate that the individual has escaped from a correctional institution or lawful custody.[45]

iii. Research

Public Health entities, along with universities and other similar organizations, may conduct research that is impacted by the Privacy Rule.[46] The impact is both on the ability to obtain information from covered entities and the ability to use or disseminate information by covered entities or hybrid entities. The Privacy Rule's implications on research are explained in Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule.[47] Please refer to that document for a thorough discussion of this issue.

f. Other Relevant Provisions

The Privacy Rule contains several other provisions addressing the use and release of PHI that are relevant to a municipality's day-to-day operations. These provisions include, but are not limited to, the following.

i. Employment-Related Issues

In general, employment records (such as personnel files) are not covered by the Privacy Rule because their creation and maintenance is not a covered function, i.e., it is not the creation or maintenance of the records that makes entities health care providers, health care plan providers, or clearinghouses. Thus, state public records laws rather than HIPAA govern the release of employment records maintained by a city. Likewise, requiring information on sick leave forms when an employee is absent does not violate HIPAA.

Note, though, that in order to *obtain* medical records from a physician or hospital, such as the results of a pre-employment physical, the covered entity (in this case the doctor or hospital) will need an authorization from the individual allowing the information to be released to the employer. Employment could be conditioned on receiving such information.

HIPAA does contain specific provisions regarding the release of PHI for workers' compensation purposes[48] and when OSHA or a similar law requires medical

[45] *See* 45 CFR §164.512(j); *see also* 45 CFR §165.501 for definitions of correctional institution and lawful custody.
[46] *See generally* 45 CFR §164.512(i).
[47] NIH Publication No. 03-5388.
[48] 45 CFR §164.512(l).

monitoring.[49] These provisions should be read, along with helpful dialogue in the preamble to the Privacy Rule, to more fully understand the provisions.

ii. Business Associate Issues

HIPAA's Privacy Rule applies both to covered entities and to their "business associates."[50] Business associates are agents, contractors, or others hired to do work for, or do the work of, covered entities, and which work requires the use or disclosure of PHI. For instance, a municipality's may enter into contracts for nursing services at its clinics. Those nurses would be considered business associates.

Your business associates must provide satisfactory assurances that they will safeguard the PHI and limit its use and disclosure. These assurances are usually provided in the form of contractual provisions.

iii. Interaction with State Law

The Privacy Rule provides a minimum level of protection for PHI. To the extent that any state law provides more stringent provisions on the release of PHI, then the more stringent law applies.[51]

Likewise, in many instances you must analyze relevant state and federal law to ascertain whether the release of PHI under a HIPAA exception is authorized. HIPAA generally *allows for* the release of PHI, it does not *mandate* the release. For instance, state and federal laws governing the reporting of diseases will dictate whether PHI can be released under the public health provisions of HIPAA.

IV. MINIMUM NECESSARY STANDARD

Several provisions regarding the release of PHI also specifically address the amount and type of PHI that can be released under those provisions.[52] In the absence of such specific direction, HIPAA requires that the minimum amount of information necessary to fulfill the purpose of the request be released.

Similarly, only those individuals who need to know PHI within the covered entity (or covered component for a hybrid entity) should have access to the PHI. Likewise, when a covered entity requests PHI from another covered entity, it

---

[49] 45 CFR §164.512(b)(1)(v).

[50]

[51] *See* 45 CFR §§160.201 – 205 for a general discussion on the interaction of state and federal provisions with HIPAA.

[52] *See, e.g.,* 45 CFR §164.512(f)(2)(i)(listing the information that may be released in order to identify or locate a suspect, fugitive, material witness or missing person).

must request the minimum amount of information necessary to fulfill its need. Collectively, these requirements fall under the "minimum necessary" standard provision of the HIPAA Privacy Rule.[53]

The minimum necessary standard does not apply to uses or disclosures of PHI for treatment purposes, to the individual whose PHI is at issue, to anyone pursuant to a valid authorization, to Health and Human Services during HIPAA enforcement investigations, or those uses and disclosures required by law (so long as the use or disclosure complies with the requirements of the law.[54]

V. CONCLUSION

Compliance with the HIPAA Privacy Rule is a time-consuming endeavor. Identifying those components of your municipality that are covered, establishing policies and procedures with those components, ensuring compliance with personnel issues such as naming a privacy officer and conducting training, and addressing the day-to-day uses and releases of PHI is challenging.

There are many resources available to aid in your compliance efforts. The U.S. Department of Health and Human Services has guidance documents available on-line, including Frequently Asked Questions. The CDC's guidance on public health related issues, authored in concert with HHS, is a useful tool (Morbidity and Mortality Weekly Report, April 11, 2003). The NIH document regarding HIPAA-related research issues is also very useful (NIH Publication Number 03-5388). Finally, the preamble to the final Privacy Rule, although voluminous, sheds light on the nuances of this very complex rule. These resources should be utilized and checked regularly for updates.

[53] 45 CFR §164.502(b).
[54] 45 CFR §164.502(b)(2); *see also* 45 CFR §164.514(d)(specifics of minimum necessary standard).