HEALTH LAW

Number 80 September 2003

THE HIPAA PRIVACY RULE: USING AND DISCLOSING HEALTH INFORMATION FOR PUBLIC HEALTH PURPOSES

■ Aimee N. Wall*

Health care providers and health insurers are required to comply with a complex new federal regulation governing the confidentiality of health information. The regulation, commonly referred to as the HIPAA Privacy Rule,[1] specifies in detail when a covered entity, such as a health care provider or health insurer, may use and disclose "protected health information" or "PHI." The complexity of this new regulation has created some confusion within the health care community. Many providers and insurers are unclear as to when they may use and disclose PHI for various purposes. In order to ensure that critical public health activities and services continue, it is important that regulated entities understand when they may use or disclose PHI for public health purposes.

This bulletin asks a series of questions intended to assist covered entities in evaluating whether a use or disclosure for public health purposes is permitted by the HIPAA Privacy Rule. It not only examines the provisions specifically targeted to what the Rule describes as public health activities, such as public health surveillance, but also other provisions of the Rule that may affect the broad array of public health services and functions, including the provision of health care and the conduct of

* The author is an Institute of Government faculty member who specializes in public health law.

1. "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, sections 262 and 264 (codified at 42 U.S.C. §§ 1320d-1329d-8). The HIPAA Privacy Rule was promulgated by the U.S. Department of Health and Human Services and is found at 45 C.F.R. Parts 160 and 164. The version of the Privacy Rule in the current (2002) version of the Code of Federal Regulations was slightly modified in 2003. *See* 68 Fed. Reg. 8,334 (Feb. 20, 2003).

School of Government
University of North Carolina at Chapel Hill
Institute of Government
Master of Public Administration Program

research. It also highlights some of the other key provisions of the Privacy Rule that come into play when an entity uses or discloses PHI, such as the requirement relating to an accounting for disclosures. Note that this bulletin is not intended to be a summary of the entire Privacy Rule. Rather, it is intended to provide a tool for covered entities to rely on when deciding whether they may use or disclose PHI for public health purposes.

What is the HIPAA Privacy Rule?

As part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress directed the U.S. Department of Health and Human Services (DHHS) to draft a regulation governing the privacy of individually identifiable health information. DHHS released the final version of the HIPAA Privacy Rule in August 2002[2] and required the health care industry to comply with the new law by April 2003.

The Rule applies to certain types of information and certain types of entities. It governs "protected health information" or PHI, which is basically any information related to health which can be identified with a particular individual.[3] The Rule regulates the use or disclosure of PHI by "covered entities." The term "covered entity" includes three types of entities: health care clearinghouses, health plans, and most health care providers.[4] A covered entity may use and disclose PHI only when permitted by the Privacy Rule.

Usually, a covered entity needs an individual's permission to disclose PHI. However, the rule allows a covered entity to disclose PHI without the individual's permission in some circumstances. For example, a covered entity may disclose PHI without the individual's permission when the disclosure is required by law.[5]

2. Standards for the Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002).

3. *See* 45 C.F.R. § 160.103 (definitions of health information, individually identifiable health information, and protected health information).

4. 45 C.F.R. § 160.103. A health care provider is a covered entity only if it transmits health information in electronic form in connection with a transaction regulated by HIPAA, such as the electronic transmission of a health insurance claim.

5. When this bulletin states that a covered entity is allowed to use or disclose PHI "without permission," this means that the entity is not required to obtain a consent or authorization or provide the individual with an opportunity to agree or object to the use or disclosure.

When evaluating whether a use or disclosure for public health purposes is permitted by the HIPAA Privacy Rule, a covered entity should ask itself whether the use or disclosure of PHI fits into any of the Rule's categories of allowable uses and disclosures. For example, is the use or disclosure required by law? Is the use or disclosure for public health activities? Is the use or disclosure necessary to avert a serious threat to health or safety? Each of the categories of allowable uses and disclosures in the Rule specifies (1) the purpose for which PHI may be used or disclosed, (2) any conditions that apply to the use or disclosure and, (3) who may use or receive the PHI. Therefore, when evaluating whether to use or disclose PHI in a specific circumstance, covered entities must ensure that the use or disclosure is consistent with all applicable requirements.

This bulletin identifies several of the categories into which a use or disclosure for public health purposes might fall and discusses how each of these categories will work in practice. The questions posed in this bulletin might be used as a checklist by a covered entity when evaluating whether to use or disclose PHI for public health purposes.

Is the Entity Required by Law to Use or Disclose PHI?

Some uses and disclosures for public health purposes are required by other federal, state, or local law. The HIPAA Privacy Rule specifically permits covered entities to use or disclose PHI when they are required to do so by other law.

The "required by law" provision of the Privacy Rule is perhaps the most straightforward section of the Rule. In sum, the provision states that if a law *requires* a covered entity to use or disclose PHI—even without the patient's permission—the Privacy Rule *permits* the covered entity to comply with such law.[6] Given that the use or disclosure is mandated by other law, the covered entity does not have any discretion in this situation. It must use or disclose the PHI as required by the other law.

The Privacy Rule also states that when the entity uses or discloses the PHI, the use or disclosure must comply with and be limited to the relevant requirements of the applicable law. This additional language in the Rule does not impose new restrictions on the covered entity, however, because the entity's use or disclosure of PHI would have been limited by the terms of the pre-existing legal requirement.

6. 45 C.F.R. § 164.512(a).

In order for a use or disclosure to be "required by law" it must be made pursuant to "a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law."[7] Legal mandates requiring use or disclosure of PHI may be based upon federal or state statutes, federal and state regulations, county ordinances, board of health rules, court orders, and subpoenas issued by a court (or other similar judicial or administrative body).[8]

There are no magic words in a statute or regulation that will make the use or disclosure "required by law." Most statutes, however, use similar language to mandate a use or disclosure—such as "shall" and "must." A statute or regulation might also provide that an official "may demand" or "may obtain" records or information. It could be argued that this type of language is not a mandate compelling use or disclosure because the official may or may not exercise his or her right to request information. However, if the official exercises his or her statutory or regulatory right to demand or obtain information, the person from whom the information is requested is required by law to comply with the official's request. Therefore, a use or disclosure pursuant to such statutory or regulatory language would be permitted by the Privacy Rule as one that is "required by law."

A few examples of public health related state statutes that clearly meet the "required by law" standard include:

- *General authority of NC DHHS Secretary*: "The Secretary *shall have the authority*…to obtain…a copy of a summary of pertinent portions of privileged patient medical records deemed necessary for investigating a disease or health hazard that may present a clear danger to the public health."[9] Another state statute permits the Secretary to delegate this authority to another person, including the State and local health directors.[10]
- *Communicable disease reporting*: "A physician licensed to practice medicine who has reason to suspect that a person about whom the physician has been consulted professionally has a communicable disease or communicable condition declared by the Commission [for Health Services] to be reported, *shall report* information required by the Commission to the local health director of the county or district in which the physician is consulted."[11]
- *Communicable disease investigation:* "Physicians and persons in charge of medical facilities or laboratories *shall, upon request and proper identification, permit* a local health director or the State Health Director *to examine, review, and obtain a copy* of medical records in their possession or under their control which pertain to the diagnosis, treatment, or prevention of a communicable disease or communicable condition…."[12]
- *Immunization*: "Immunization certificates and information concerning immunizations contained in medical and other records *shall, upon request, be shared* with the Department [of Health and Human Services], local health departments, and the patient's attending physician."[13]
- *Bioterrorism*: "The State Health Director may issue a temporary order *requiring* health care providers to report symptoms, diseases, conditions…when necessary to conduct a public health investigation or surveillance of an illness, condition or health hazard that may have been caused by a terrorist incident…."[14] The State Health Director and local health directors also "*may examine, review, and obtain* a copy of records containing confidential or protected health information"

7. 45 C.F.R. § 164.103.

8. It is important to note that the definition of "required by law" does not include as an example subpoenas not issued by a court (such as a subpoena issued by an attorney). Because of North Carolina's physician-patient privilege statute (N.C. Gen Stat. § 8-53 (hereinafter G.S.)), covered entities should proceed with caution when disclosing PHI in response to a subpoena not issued by a court. For more information, *see* Jill Moore, "Responding to Subpoenas for Health Information: Guidance for Local Health Departments" (Oct. 2002), *available at* http://www.medicalprivacy.unc.edu.

9. G.S. § 130A-5(2) (emphasis added).

10. G.S. § 130A-6.

11. G.S. § 130A-135 (emphasis added)

12. G.S. § 130A-144(b) (emphasis added)

13. G.S. § 130A-153(c) (emphasis added)

14. G.S. § 130A-476(b) (emphasis added). Note that disclosure under this provision would only impose a duty on covered entities once the State Health Director issues the temporary order.

that relate to either a mandatory or a voluntary report.[15]

- *Cancer registry*: "All health care facilities and health care providers that detect, diagnose, or treat cancer *shall report* to the central cancer registry each diagnosis of cancer…."[16]
- *Birth defects monitoring program:* "Physicians and … medical facilities *shall, upon request, permit staff* of the [Birth Defects Monitoring Program] *to examine, review and obtain a copy* of any medical record in their possession or under their control that pertains to a diagnosed or suspected birth defect, including the records of the mother."[17]
- *Birth and death registration*: State statutes require births and deaths to be registered with the local health department.[18] The statutes specify the content of the birth and death certificates, including the medical information that must be furnished by physicians, medical facilities and others.[19]

A covered entity subject to one of the above statutes would be required by law to use or disclose PHI for public health purposes and therefore must use or disclose it consistent with the state law requirement.

In three specific circumstances, the Privacy Rule imposes additional conditions on a use or disclosure "required by law":

- when an entity is disclosing PHI to a government authority, such as a local department of social services, regarding an individual whom the entity reasonably believes to be a victim of abuse, neglect, or domestic violence (except for reports of child abuse and neglect);[20]
- when an entity is disclosing PHI in the course of judicial and administrative proceedings;[21] and
- when an entity is disclosing PHI for law enforcement purposes.[22]

If the entity is required by law to use or disclose PHI and the use or disclosure falls within any of the above three circumstances, the entity should consult the Rule and other applicable law to ensure that it is complying with all conditions applicable to such use or disclosure.

Is the Entity Using or Disclosing PHI for Public Health Activities?

In drafting the Privacy Rule, DHHS recognized that in many instances a use or disclosure for public health purposes would not be "required by law" but that the activity was important enough that the use or disclosure should be allowed without the patient's permission. Therefore, the agency created a separate category of the Rule that addresses when a covered entity may use or disclose PHI for public health activities without the patient's permission.[23] DHHS expressed a clear intention to preserve access to information for public health activities.[24] The agency explained that terms used in the public health activities categories "would be intended to cover the spectrum of public health activities carried out by federal, State, and local public health authorities…."[25]

The "public health activities" category breaks these activities down into five general subcategories:

- prevention and control of disease, injury and disability;
- communicable disease notification;
- child abuse and neglect reporting;
- FDA-regulated product or activity monitoring; and
- work-related illness or injury monitoring and workplace medical surveillance.

---

15. G.S. § 130A-476(c) (emphasis added). For a full discussion of the HIPAA implications of this provision and others included in the recent state bioterrorism legislation, *see* Jill Moore, Appendix, "New North Carolina Public Health Bioterrorism Law," Health Law Bulletin No. 79 (Feb. 2003).

16. G.S. § 130A-209(a) (emphasis added).

17. G.S. § 130A-131.16 (emphasis added).

18. G.S. § 130A-101 et seq. (birth); G.S. § 130A-115 et seq. (death)

19. *Id.*

20. 45 C.F.R. § 164.512(c)

21. 45 C.F.R. § 164.512(e)

22. 45 C.F.R. § 164.512(f)

23. 45 C.F.R. § 164.512(b).

24. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, Guidance from the DHHS Office of Civil Rights 80 (Dec. 3, 2002), *available at* http://www.hhs.gov/ocr/hipaa/privacy.html; Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,917, 59,956 (Nov. 3, 1999).

25. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,917, 59,956 (Nov. 3, 1999).

For each of these subcategories, this bulletin summarizes (1) the purpose for which a covered entity may use or disclose PHI and any conditions that apply to such a use or disclosure and (2) to whom the entity may disclose the PHI. This bulletin then includes a discussion of relevant North Carolina law where appropriate.

Prevention and Control

Purposes

A covered entity may use or disclose PHI for the core public health purposes of preventing or controlling disease, injury, or disability. The Rule expands on these core purposes by explaining that they include, but are not limited to:

- disease and injury reporting;
- birth and death reporting; and
- the conduct of public health surveillance, public health investigations, and public health interventions.

The reporting, investigation and intervention provisions described above are generally self-explanatory. The term "public health surveillance," though, may not be well understood in the private sector. The Centers for Disease Control explain that surveillance "is a term describing a method for public health data collection" which may "involve the regular, ongoing collection and analysis of health-related data conducted to monitor the frequency of occurrence and distribution of disease or a health condition in the population."[26] An example of public health surveillance would be ongoing collection of data on childhood obesity throughout a community.

Recipients

Covered entities may make disclosures for the prevention and control purposes described above to two types of officials or organizations: public health authorities and certain foreign government agencies. First, an entity may disclose PHI to a "public health authority" that is authorized by law to collect or receive information for the prevention and control purposes described above.[27] The term "public health authority" is defined in the Rule to mean "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe … that is responsible for public health matters as part of its official mandate."[28] The term may also include "a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority."[29] Therefore, in some limited circumstances, a private person or organization may be a "public health authority" if it has been granted authority by a public agency.

It is important to note that the term "public health authority" has an entirely different meaning under the Privacy Rule than under North Carolina law.[30] When evaluating whether they are disclosing PHI to a "public health authority" for the purpose of complying with the Privacy Rule, covered entities should rely *only* on the definition used in the Rule. Depending on the circumstances, the term "public health authority" (as the term is used in the Privacy Rule) may include the following organizations and individuals:

- *Federal*: Components and officials of the U.S. Department of Health and Human Services including those within the Centers for Disease Control and the Food and Drug Administration
- *State*: Components and officials of the N.C. Department of Health and Human Services, the N.C. Department of Environment and Natural Resources, and the N.C. Department of Agriculture as well as parallel agencies in other states.
- *Local*: Components and officials of local health departments and boards of health. Other non-traditional public health authorities might include a county sheriff's office or a private, non-profit organization that is responsible for animal control activities, such as rabies control.

26. Centers for Disease Control, "Guidelines for Defining Public Health Research and Public Health Non-Research" (Oct. 4, 1999), *available at* http://www.cdc.gov/od/ads/opspoll1.htm.

27. If the covered entity is also a public health authority, it may use the PHI for prevention and control purposes.

28. 45 C.F.R. § 164.501.

29. *Id*.

30. In North Carolina, the term "public health authority" refers to a legal entity that is created for the specific purpose of providing public health services in a defined geographical area. *See* G.S. § 130A-45 *et seq*.

In addition to "public health authorities," covered entities may also disclose PHI to an official of a foreign government agency that is acting in collaboration with a public health authority. A covered entity may disclose PHI to such an official only if it is directed to do so by the public health authority. For example, if the U.S. Centers for Disease Control (CDC) is collaborating with public health officials in Canada while investigating a disease outbreak, a covered entity could disclose PHI to a Canadian government agency if CDC directs the entity to do so.

Discussion

In many instances, covered entities will be "required by law" to use or disclose PHI for these prevention and control purposes and therefore the entity need not even consider the applicability of this subcategory. However, in other instances, a law may simply *permit* or *authorize* a use or disclosure. For example:

- *Communicable disease reporting:* As discussed above, physicians are *required* by state law to report certain communicable diseases. Medical facilities, on the other hand, are only *permitted* to file such reports. The statute provides that a "medical facility in which there is a patient reasonably suspected of having a communicable disease or condition declared by the Commission to be reported, *may* report information…to the local health director of the county or district in which the facility is located."[31]
- *Bioterrorism:* As discussed above, the State Health Director may issue a temporary order *requiring* reporting related to bioterrorism. But North Carolina law also *permits* providers, health care facilities or units of State or local government to report to the State Health Director or a local health director any events that may indicate the existence of a case or outbreak of an illness that may have been caused by bioterrorism even when the State Health Director has not issued a temporary order.[32] State law also *permits* hospitals and urgent care centers to participate in a program for reporting emergency department data to a program established by the State Health Director for public health surveillance purposes.[33]
- *Health statistics:* The State Center for Health Statistics is authorized to collect, maintain and analyze health data for various health-related research purposes. The Center could establish a new registry to track a specific disease. The Center is only permitted, however, to collect health data on a *voluntary* basis. It is not authorized to compel mandatory reporting.[34]

Before using or disclosing PHI under this public health subcategory when the disclosure is not otherwise required by law, the covered entity must determine whether it will be using or disclosing PHI (a) for the "purpose of preventing or controlling disease, injury, or disability" and (b) to an appropriate recipeent. In all three of the examples described above, both prongs of this test are clearly satisfied and therefore a covered entity is permitted to use or disclose PHI as authorized by those laws.

Communicable Disease Notification

Purpose and Conditions

In addition to being able to use PHI or disclose PHI to public health authorities and others for prevention and control purposes, the Privacy Rule also permits covered entities to use and disclose PHI without the patient's permission in order to notify an individual that he or she may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease.[35] A covered entity may make such a notification only if the entity is authorized by law to notify the person as necessary in the conduct of a public health intervention or investigation.

Recipients

Under this provision, covered entities may disclose PHI only to individuals that may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.[36]

31. G.S. § 130A-137.

32. G.S. § 130A-476(a). Note that the state law also provides that "To the extent practicable, a person who makes a report under this subsection shall not disclose personally identifiable information." *Id*.

33. G.S. § 130A-476(f).

34. G.S. § 130A-373.

35. 45 C.F.R. § 164.512(b)(iv).

36. Throughout this section, a reference to communicable diseases should also be interpreted to encompass communicable conditions.

Discussion

As explained above, a covered entity may use and disclose PHI without the patient's permission in order to notify potentially exposed or at-risk individuals only if the entity is *authorized by law* to make such a notification in the conduct of a public health intervention or investigation. In North Carolina, public health officials are clearly authorized by law to make such notifications with respect to communicable diseases. Other providers, such as private physicians, also appear to have some limited authority to make such notifications in certain situations. Therefore, communicable disease notifications will be permitted under the Privacy Rule in many instances. For almost all such notifications, however, state confidentiality law prevents the disclosure of the identity of the source of the exposure or potential exposure.

The authority of public health officials to notify exposed or potentially exposed individuals relies on a combination of legal authorities granted to various public health bodies and officials:

- State and local health directors have broad general authority to investigate, prevent, and control communicable diseases and to protect the public health.[37]
- The Commission for Health Services (the Commission) is required to adopt rules that identify communicable diseases that must be reported and to prescribe the "control measures" that must be followed for each disease in order to protect the public health (such as testing, treatment, or quarantine).[38]
- Local health directors have the duty to investigate cases of reportable communicable diseases and to ensure that the control measures required by the Commission are followed.[39]

In general, the duty to notify exposed individuals is inherent in the broad powers of the State and local health directors because such notification is necessary to protect the public health. More specifically, many of the "control measures" required by the Commission require public health officials to notify certain individuals who may have been exposed to or may be at risk for contracting or spreading a communicable disease. For example, individuals infected with certain sexually transmitted diseases (including syphilis) must give the State the names of sexual partners and others so that the State may notify, test, and treat those persons as appropriate and necessary.[40] Therefore, public health officials in North Carolina who are also "covered entities" under the Privacy Rule will clearly be permitted to notify potentially exposed or at-risk individuals.

Other providers, such as private physicians, may be required to report communicable diseases but they do not have the same clear statutory or regulatory authority to control communicable diseases and notify contacts.[41] The current rules of the Commission do, however, specifically require attending physicians to notify contacts in some instances. For example, the rules governing HIV control measures require an attending physician to either notify the spouse of an HIV-infected patient (with the patient's consent) or inform the state Division of Public Health so that the State may notify the spouse.[42] In addition, other rules authorize attending physicians to disclose limited information to the physician of a person who has been or may have been exposed to HIV or Hepatitis B as the result of an accidental exposure to blood or body fluids, such as an accidental needlestick.[43] Therefore, in those limited circumstances in which a health care provider (other than the State or local health director) has specific authority to notify an individual, the

37. G.S. § 130A-5(2) (authority of Secretary of DHHS which is generally delegated to the State Health Director pursuant to G.S. § 130A-6); G.S. § 130A-41(b)(authority of local health director)

38. G.S. § 130A-134; G.S. § 130A-147.

39. G.S. § 130A-144(e).

40. 10A NCAC 41A. 0204(c)(3). *See also* 10A NCAC 41A.0205 (requires the local health director to investigate tuberculosis cases and test certain persons who had contact with those cases); 10A NCAC 41A. 0202(13) (requires DHHS to establish a program for notification and counseling of partners of individuals infected with HIV).

41. Note that physicians are required to report; facilities are permitted to report. G.S. § 130A-135; G.S. § 130A-137.

42. 10A NCAC 41A. 0202(2)(b).

43. If a person has had a non-sexual exposure to the blood or bodily fluids of another person (for example, as the result of an accidental needlestick) and the exposure would pose a significant risk of transmitting HIV if the person who is the source of the blood or fluids was infected with HIV, the attending physician of the person who is the source of the blood or fluids may notify the attending physician of the person who may have been exposed about the HIV status of the source. 10A NCAC 41A. 0202(4). A similar notification requirement applies with respect to non-sexual exposure (or potential exposure) to Hepatitis B. 10A NCAC 41A. 0202(4) and 41A. 0203(b)(3).

provider is permitted under the Privacy Rule to make such a notification. In all other instances, the provider should obtain the patient's written authorization prior to directly notifying a potentially exposed or at-risk individual.

With respect to almost any notification related to a reportable communicable disease, the notification should *not* reveal the identity of the source of the exposure or potential exposure. Despite the fact that the Privacy Rule would likely permit the disclosure of the source's identity, North Carolina has a strict confidentiality statute that protects all information that identifies a person who has or may have a reportable communicable disease.[44] This confidentiality statute is "more stringent" than the Privacy Rule so covered entities must continue to comply with the state law rather than the Rule. Therefore, unless the person making the notification has the specific written consent of the source of the exposure or potential exposure, the notification should only reveal that exposure has or may have occurred. It should not reveal the name of the source.

Child Abuse and Neglect Reporting

Purposes

A covered entity may use or disclose PHI in order to report child abuse or neglect.

Recipients

The entity may only make such a disclosure to a "public health authority or other appropriate government authority authorized by law" to receive reports of child abuse and neglect.[45]

Discussion

Under North Carolina law, suspected child abuse, neglect, dependency or death due to maltreatment by a caretaker must be reported to the department of social services in the county where the child either lives or is found.[46] The state statute is quite broad; it applies to "any person or institution who has cause to suspect that any juvenile is abused, neglected, or dependent…or has died as the result of maltreatment."[47] It is important to note that the state law is more expansive than the Privacy Rule because it requires reporting of not only abuse and neglect, but also dependency and death due to maltreatment.[48] The state law specifies that certain health information must be included in the report (if known to the person making the report), including "the nature and extent of any injury or condition resulting from abuse, neglect, or dependency."

Because reports of child abuse, neglect, dependency and death due to maltreatment are required by law, it is unnecessary for covered entities to evaluate whether the reports would be permitted under the "public health activities" provisions of the Privacy Rule.[49] Covered entities are clearly permitted to make these reports under the Privacy Rule and, because reporting is *required* by state law, covered entities *must* make such reports.

---

44. G.S. § 130A-143

45. 45 C.F.R. § 164.512(b)(ii). In North Carolina and in many other states, these types of reports are made to departments of social services agencies rather than to public health authorities. However, in drafting the Privacy Rule, DHHS elected to include this category of disclosures under the umbrella of "public health" because, in the original legislation, Congress included specific language that grouped public health activities together with child abuse and neglect reporting. "Because HIPAA addresses child abuse specifically in connection with a state's public health activities, we believe it would not be appropriate to include child abuse-related disclosures in this separate paragraph on abuse." 65 Fed. Reg. 82,462, 82,527 (Dec. 28, 2000). DHHS inferred that it was the intent of Congress to categorize child abuse and neglect as a public health activity. In a separate section of the Rule, DHHS permits covered entities to disclose PHI without the patient's permission for other types of abuse, neglect and domestic violence, such as spousal or elder abuse (see discussion below). *See* 45 C.F.R. § 164.512(c).

46. G.S. § 7B-301.

47. *Id*.

48. *Id*. A "dependent juvenile" is a juvenile in need of assistance or placement because he or she "has no parent, guardian, or custodian responsible for [his or her] care or supervision or whose parent, guardian, or custodian is unable to provide for the care or supervision and lacks and appropriate alternative child care arrangement." G.S. § 7B-101(9).

49. *See* John Saxon, "Confidentiality and Social Services (Part V): The HIPAA Privacy Rule and County Departments of Social Services," Social Services Bulletin No. 38 (Aug. 2003), *available at* http://www.medicalprivacy.unc.edu.

FDA-Regulated Product or Activity Monitoring

Purposes

A covered entity may use or disclose PHI for activities related to the quality, safety or effectiveness of an FDA-regulated product or activity.[50]

The Rule includes several examples of such activities:

- collecting or reporting adverse events, product defects or problems, or biological product deviations;
- tracking FDA-regulated products;
- enabling product recalls, repairs, or lookback;
- conducting post-marketing surveillance.

Recipients

A covered entity may disclose PHI under this provision to a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility.[51]

This category of recipients is slightly different from the categories described in previous sections because it is broad enough to include private sector organizations, such as pharmaceutical companies and medical device manufacturers. DHHS explained: "We note that under this provision, a covered entity may disclose protected health information to a non-governmental organization without individual authorization for inclusion in a private data base or registry…."[52] DHHS explained that the FDA relies upon voluntary reporting that is channeled through many of these private organizations and that the Privacy Rule should not impede these voluntary reports.[53]

Work-Related Illness or Injury Monitoring and Workplace Medical Surveillance

Purpose and Conditions

The Privacy Rule includes workplace surveillance and work-related illnesses and injuries within the category of public health activities. The Rule permits a limited class of covered entities to make disclosures of PHI to an employer if three conditions are satisfied.

The Rule only authorizes covered health care providers (not health plans or health care clearinghouses) to make such disclosures if the provider either is a member of the employer's workforce or provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury.

The provider may make such disclosures only if all of the following conditions are satisfied:

- The PHI that is disclosed consists of findings concerning a work-related illness or injury or workplace-related medical surveillance.
- The employer needs such findings in order to comply with its obligations under the regulations governing the Occupational Safety and Health Administration[54] or the Mine Safety and Health Administration[55] or under state law having a similar purpose, to record such illness or injury or to carry out workplace medical surveillance.
- The provider gives the individual written notice that PHI relating to medical surveillance of the workplace and work-related illness and injuries is disclosed to the employer.

The written notice requirement may be satisfied in two ways. The provider may give a copy of the notice directly to the individual at the time the health care is provided or, if the health care is provided on the work site of the employer, the provider may post the notice in a prominent place at the location where the health care is provided.

Recipients

A covered health care provider may disclose PHI to an employer in the above circumstances if the individual who is the subject of the information is a member of the employer's "workforce." The term "workforce" is defined broadly to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the covered entity, is under

50. 45 C.F.R. § 164.512(b)(iii).
51. *Id*.
52. 65 Fed. Reg. at 82,462, 82,526 (Dec. 28, 2000).
53. 67 Fed. Reg. at 53,182, 53,227 (Aug. 14, 2002).
54. 29 CFR parts 1904-1928.
55. 30 CFR parts 50-90.

the direct control of such entity, whether or not they are paid by the covered entity."[56]

Is the Entity Using or Disclosing PHI In Order To Avert a Serious Threat to Health or Safety?

The Privacy Rule includes a fairly broad provision that allows a covered entity to disclose PHI when there is an apparent threat to health or safety. An entity may use or disclose PHI if the entity in good faith believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[57] The Rule explains that it is presumed that the covered entity acted based upon a "good faith belief" if the entity's belief is based upon either the entity's actual knowledge or a credible representation by a person with apparent knowledge or authority.[58] In addition to the "good faith belief" standard, the Rule also provides that such a disclosure must be "consistent with applicable law and standards of ethical conduct."

A covered entity may make a disclosure under this provision only to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.[59] This provision is not limited to public health but there certainly could be a situation in which a disclosure to a public health official would be appropriate.

Is the Entity Using or Disclosing PHI for the Purposes of Treatment, Payment or Health Care Operations?

All local health departments in North Carolina act as health care providers as well as serving their communities as local public health officials. Most provide various types of direct health care services (such as immunizations) and operate health care clinics (such as prenatal clinics). In some instances, they also collect payment for those health care services. Therefore, a covered entity may be asked to disclose PHI to a local health department for purposes related to the department's "treatment" of a patient, "payment" for such treatment, or for the department's "health care operations."[60]

Under the Privacy Rule, a covered entity is allowed to use or disclose PHI to other persons or entities for the purposes of treatment, payment and health care operations (TPO) without the patient's written permission as follows:

- The entity may use or disclose PHI for its own TPO.
- The entity may disclose PHI for treatment activities of a health care provider.
- The entity may disclose PHI to another covered entity or a health care provider for the payment activities of the recipient.
- The entity may disclose PHI to another covered entity for health care operations of the recipient if the following three conditions are satisfied: (1) both entities either have or had a relationship with the patient; (2) the PHI pertains to such relationship; and (3) the disclosure is for one of several limited health care operations activities, including quality improvement, training, and fraud and abuse detection and compliance.
- If the entity is participating in an "organized health care arrangement," it may disclose PHI to another entity in the arrangement for health care operations activities of the arrangement.[61]

56. 45 C.F.R. § 160.103.
57. 45 C.F.R. § 164.512(j).
58. 45 C.F.R. § 164.512(j)(4).
59. 45 C.F.R. § 164.512(j)(1)(i).

60. "Treatment" means "the provision, coordination, or management of health care and related services by one or more health care provider, including the coordination or management of health care by a health care provider with a third part; consultation between health care providers relating to a patient; or the referral of a patient for health care from on health care provider to another." 45 C.F.R. § 164.501. The definition of "payment" includes activities undertaken by a "health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits" or by a "health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id*. The term "health care operations" is defined generally to refer to the internal operations of a health plan or health care provider and includes activities such as quality assessment and improvement, evaluating and training practitioners, business management and administration. *Id*. *See also* Mark Botts, "Using and Disclosing Information for Treatment, Payment and Health Care Operations" (Oct. 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/UpTPO.pdf.

61. 45 C.F.R. § 164.506(c). An "organized health care arrangement" is generally an arrangement where two or more

Each of the TPO provisions discussed above approaches the issue of intended recipients differently. Under the first provision, the Privacy Rule permits a covered entity to disclose PHI for its own TPO activities to anyone. Under the second provision, a covered entity may disclose PHI for treatment activities of a health care provider. The Rule does not specifically state, however, that the disclosure must be *to* that other health care provider. A situation could arise in which one provider is asked by a second provider to disclose PHI to a third party in order to support the second provider's treatment of a mutual patient. For example, one provider might ask another provider to send information to a laboratory. The Privacy Rule appears to permit such a disclosure. The third, fourth and fifth provisions specifically identify the intended recipients.

While the Privacy Rule allows uses and disclosures for TPO without the patient's permission, state or other federal law may require written permission. In general, if a state law is more protective of a patient's privacy than the Privacy Rule—such as by requiring consent when the Rule would not—the state law must be followed (see discussion of preemption on page 13). For example, North Carolina has a strict state law governing the confidentiality of information relating to a person who has or may have a reportable communicable disease or condition.[62] This law permits disclosure of communicable disease information for treatment purposes,[63] but it does not permit disclosure for many other purposes including payment and health care operations. Therefore, when a covered entity in North Carolina wishes to release communicable disease information for payment or health care operations, the entity must obtain written permission (or "consent") from the patient or the patient's personal representative.[64]

covered entities are clinically integrated or participate in joint activities, such as utilization review or payment activities. 45 C.F.R. § 160.103.

62. G.S. § 130A-143

63. *Id*. (allowing disclosure "to health care personnel providing medical care to the patient").

64. *See* Jill Moore and Aimee Wall, "Using and Disclosing Patients' Health Information for Treatment, Payment, and Health Care Operations: Recommendations for North Carolina Local Health Departments" (Dec. 19, 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/LHDTPOrecs.pdf.

Is the Entity Using or Disclosing De-Identified Information?

The Privacy Rule only applies to "identifiable" information.[65] Therefore, an entity is free (under the Rule) to disclose "de-identified" information for public health or any other purposes at any time.

The Rule outlines two methods for de-identifying information.[66] First, information may be considered de-identified if all unique identifying numbers, characteristics or codes have been removed, including 17 specific identifiers (including name, address, social security number, and medical record number). In addition, the entity disclosing the information must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual.

The second method for de-identifying information is to have a statistical expert determine that the "risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual."[67] The covered entity must document the expert's methods and analysis.

Under the Privacy Rule, a covered entity may disclose de-identified information to anyone without limitation. Note that other law may impose more stringent requirements on the entity's use or disclosure of the information.

Is the Entity Using or Disclosing a "Limited Data Set"?

Public health officials do not always need to know a person's name, address and social security number in order to conduct public health surveillance, but the de-identification requirements provided in the Privacy Rule may be too rigid in some circumstances. Some argue that the data becomes relatively worthless for public health purposes when all of the identifiers have been removed as required by the Rule. For example, without zip codes and other geographic identifiers, it is impossible to track the spread of an illness throughout a city, state or region. As an alternative to the stringent de-identification standard, the Privacy Rule also permits covered entities to disclose a "limited data set" for public health purposes under some circumstances.

65. *See* 45 C.F.R. § 16.103 (definitions of individually identifiable health information and protected health information).

66. 45 C.F.R. §§ 164.502(d); 164.514(a)-(c).

67. 45 C.F.R. § 164.514(b)(1).

A "limited data set" is defined as PHI that excludes several specific identifiers.[68] The primary benefit of the limited data set over de-identified information is that *fewer* identifiers need to be removed. For example, in order for information to be "de-identified," virtually all geographic identifiers must be removed. In a limited data set, the PHI may include a town or city, state and zip code. These types of geographic identifiers can be very useful to public health officials in their surveillance activities. In addition, all dates (such as birth date, admission date, discharge date and date of death) must be removed from de-identified information whereas all dates may be retained on a limited data set.

In order for a covered entity to use or disclose a limited data set, the entity must enter into a "data use agreement" with the recipient of the data set. A data use agreement is a specific type of contractual agreement that limits the recipient's use and disclosure of the PHI. The Privacy Rule specifies the terms that must be included in the contract, such as requiring the recipient to use appropriate safeguards in protecting the information, report any inappropriate uses or disclosures and refrain from contacting the individuals who are the subjects of the information.

The rule does not specify to whom a limited data set may be disclosed. The only limitation to consider is that the disclosure must be for public health, research or health care operations purposes. Given the wide variety of activities that DHHS included under the subheading "public health"—including traditional public health activities, reporting child abuse and neglect, monitoring FDA-regulated products, and monitoring work-related illness and injury—it is likely DHHS envisioned that a limited data set could be disclosed for public health purposes to various types of public and private organizations, including state and local public health officials.

Is the Use or Disclosure Permitted Without Permission for Other Purposes?

The six broad categories of uses and disclosures described above (required by law, public health, serious and imminent threat, TPO, de-identified information, and limited data sets) will encompass most disclosures that a covered entity wishes to make or is asked to make without the patient's permission to a public health official or for public health purposes. If, however, a covered entity concludes that the use or disclosure does not fall within one of those six categories, it should also review the other categories of uses and disclosures that are permitted under the Rule before concluding that it is prohibited from using or disclosing the PHI without the patient's permission.

A few categories in particular may come into play when an entity is considering using or disclosing PHI for public health purposes. Each of these additional categories is briefly summarized below, but, as with all uses and disclosures, covered entities should refer to the specific provisions of the Privacy Rule (in conjunction with other applicable law) to determine whether the use or disclosure is permitted.

Research

The Privacy Rule outlines detailed procedures that must be followed before a covered entity may use or disclose PHI for research purposes. "Research" is defined in the Privacy Rule as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[69]

Some might argue that much of the data-gathering by public health officials is "research" in that it is a systematic investigation and it is designed to contribute to "generalizable" knowledge. Under most circumstances, however, research-like activities conducted by public health agencies will fall within the broad category of permitted disclosures for prevention and control described above, which includes public health surveillance, investigation and intervention. For example, if a hospital elects to submit PHI to the state for the pilot program collecting emergency department data for bioterrorism purposes,[70] the data would be submitted for public health surveillance purposes rather than research purposes.

In general, if a covered entity concludes that a public health official is requesting PHI that does not fall under the broad umbrella of "prevention and control" but rather is requesting PHI for "research," the entity may disclose the PHI without the individual's authorization only if it obtains specific documentation

68. 45 C.F.R. § 164.514(e)(2). Note that information that has been "de-identified" is not considered PHI and therefore is not subject to the requirements or penalties of the Privacy Rule. Information in a limited data set is still considered PHI and therefore is still subject to the Rule.

69. 45 C.F.R. § 164.501

70. G.S. § 130A-476(f).

from the official.[71] The documentation must include several specific elements, including a statement that the research proposal has been reviewed by an Institutional Review Board (IRB) or a privacy board that evaluated the potential risks to the privacy of the individuals.[72]

Government Programs Providing Public Benefits

The Privacy Rule includes a specific category that permits two government programs to share PHI in two limited circumstances. The first provision allows a *health plan* that is a government program providing public benefits (such a Medicaid or Health Choice) to share eligibility or enrollment information with another agency administering a government program providing public benefits when such information sharing is required or expressly authorized by statute or regulation.[73] The second provision permits information sharing between two covered entities that are both government agencies administering public benefits programs. Under this provision the two programs may disclose PHI to each other if:

- the programs serve the same or similar populations and
- the disclosure of PHI is necessary to coordinate the covered functions of such programs or improve the administration and management relating to the covered functions of such programs.[74]

The key to an analysis under these two provisions is determining when a public health official or agency is a "government agency administering a government program providing public benefits." Depending on a local health department's role with a particular program, a department may fall within this category with respect to certain public programs, such as the Women, Infants and Children (WIC) program, in which it performs eligibility, enrollment and other administrative functions.

71. 45 C.F.R. § 164.512(i). Different rules apply with respect to reviews preparatory to research and research on decedent's information. *See* 45 C.F.R. § 164.512(i)(1)(ii) and (iii).

72. 45 C.F.R. § 164.512(i)(2).

73. 45 C.F.R. § 164.512(k)(6)(i).

74. 45 C.F.R. § 164.512(k)(6)(ii).

Correctional Institutions

A covered entity is permitted to disclose PHI about an inmate[75] or another individual to a correctional institution[76] when the information is necessary for several specific purposes, such as providing health care to the inmate and for the health and safety of those transporting the inmate.[77] In some North Carolina counties, the local health department provides the health services at the county jail. Therefore, the local health department may be considered part of the correctional institution and a covered entity may be able to disclose PHI to the health department staff about an inmate in that jail. In this situation, the health department will not necessarily be acting in its public health role but rather will be acting as both a provider and an arm of the correctional institution.

Disaster Relief

A covered entity is allowed to use or disclose PHI in order to notify a family member or other person of an individual's location, general condition, or death. An entity may also disclose PHI to a public or private organization authorized by law or by its charter to assist in disaster relief efforts in order to coordinate any such notification.[78] It is conceivable that the State or local health department or a private public health organization could be involved in such disaster relief efforts. If so, a covered entity may disclose PHI to them under these limited circumstances. Certain additional restrictions may apply to this type of disclosure depending on whether the

75. An inmate is "a person incarcerated in or otherwise confined to a correctional institution." 45 C.F.R. § 164.501. Note that the rule specifically states that "an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody." 45 C.F.R. § 164.512(k)(5)(iii).

76. Correctional institution is defined in the rule to include any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody (such as witnesses and persons criminally committed to mental institutions). 45 C.F.R. § 164.501. The term includes facilities either operated by or under contract to a government or tribe. Id.

77. 45 C.F.R. § 164.512(k)(5)(i).

78. 45 C.F.R. § 164.510(b)(4).

individual is present or incapacitated and whether the situation is an emergency.

Does the Entity Have the Individual's Authorization?

If the use or disclosure is not otherwise permitted by the Privacy Rule, the Rule always allows a covered entity to disclose PHI to any person or organization for any purpose if the entity obtains the individual's written authorization.[79] The Rule spells out several specific requirements that must be satisfied in order for an authorization to be considered a valid authorization under the Rule.[80] For example, the authorization form must be written in plain language and include certain elements, including a description of the PHI to be disclosed, the purpose of the use or disclosure and an expiration date or event.[81]

Preemption

If a disclosure for public health purposes does not fall within any of the categories described above, the covered entity does not have the patient's authorization to make the disclosure, and it appears, therefore, that the Privacy Rule does not permit the disclosure, the entity should determine whether a specific state law permits the disclosure and, if so, whether that the Rule preempts the state law.[82]

79. 45 C.F.R. §§ 164.502; 164.508.

80. 45 C.F.R. § 164.508(b)-(c); *see also* Mark Botts, Using and Disclosing Information with Individual Permission (Oct. 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/Upprmmsn.pdf.

81. 45 C.F.R. § 164.508(c).

82. Technically, a covered entity should start any analysis of a public health disclosure with a preemption analysis. If a provision of state law permits or requires a disclosure that falls within the preemption exception, the covered entity is permitted (or required, depending on the state law) to make the disclosure. But given the almost direct overlap between the public health provisions of the Privacy Rule and the provisions of this special preemption category, a covered entity could approach its analysis from either starting point and it will likely reach the same conclusion.

General Rule of Preemption

If a state law and the Privacy Rule conflict,[83] a covered entity must evaluate whether the Rule or the state law will govern. In general, the Privacy Rule provides a "federal floor" of privacy protections to patients. This means that if a state law is *more* protective of the patient's privacy than the applicable provision of the Privacy Rule (i.e., "more stringent"[84]), the state law will not be preempted; in other words, the state law will govern. If the state law is *less* protective of the patient's privacy, the applicable provision of the Rule will preempt the provision of state law and the Rule will govern.[85]

Above and beyond this general rule, however, HIPAA identifies a few special categories of state laws that will not be preempted even if the state law is less protective of a patient's privacy than the Privacy Rule. The two categories that are of particular relevance to disclosures for public health purposes are discussed briefly below.

Public Health Exception

The Privacy Rule will not preempt a provision of state law that provides for:

- the reporting of disease or injury, child abuse, birth, or death; or
- the conduct of public health surveillance, investigation, or intervention.[86]

This exception echoes some of the provisions of the Privacy Rule that specifically focus on public health activities. For example, the Privacy Rule permits covered entities to disclose PHI to certain persons and organizations without individual permission:

83. A state law and a provision of the Privacy Rule conflict if they are "contrary" to one another. The term "contrary" is defined in the Rule to mean either "(1) A covered entity would find it impossible to comply with both the State and federal requirements; or (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full objectives of" the Administrative Simplification provisions of HIPAA. 45 C.F.R. § 160.202.

84. 45 C.F.R. § 160.202.

85. 45 C.F.R. § 160.203.

86. 45 C.F.R. § 160.203(c).

- in order to report "disease, injury, [and] vital events, such as birth or death"[87] and "child abuse and neglect;"[88] and
- for the conduct of public health surveillance, investigation, or intervention.[89]

The differences between the provisions of the Privacy Rule and this special preemption exception category are extremely subtle. For example, the Rule permits disclosures for reporting "child abuse and neglect" but the preemption exception only applies to provisions of state law relating to the reporting of "child abuse." In addition, the Rule only permits a covered entity to report child abuse and neglect to "a public health authority or other appropriate government authority authorized by law" to receive such reports. The preemption exception is not so limited: a covered entity may disclose PHI to any person or entity if the applicable provision of state law allows such a disclosure. Given these subtle differences, it is unlikely that a disclosure for public health purposes *will not* fall within the public health category of the Privacy Rule but *will* fall within the preemption exception. Covered entities should, however, be aware of this exception.

Secretarial Exception Determinations

In limited circumstances, the Secretary of DHHS may make a determination that a provision of state law that would otherwise be preempted by the Privacy Rule is excepted from preemption.[90] There are several different types of laws for which an "exception determination" may be made but only one is directly relevant to public health. The Secretary may except any provision of state law if he or she determines that the provision is necessary "for purposes of serving a compelling need related to public health, safety, or welfare" and the intrusion into privacy is warranted when balanced against the need to be served.[91] Any person may submit a request to the Secretary to have a provision of law excepted.[92]

87. 45 C.F.R. § 164.512(b)(1)(i).

88. 45 C.F.R. § 164.512(b)(1)(ii).

89. 45 C.F.R. § 164.512(b)(1)(i).

90. 45 C.F.R. § 160.203(a).

91. 45 C.F.R. § 160.203(a)(1)(iv).

92. 45 C.F.R. § 160.204(a); *see also* 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000) (explaining that the rule was modified so that requests may be submitted by any person rather than only by a State official).

Therefore, if a covered entity is confronted with a state law that would permit it to disclose PHI for public health but the Privacy Rule would *not* permit the disclosure, the entity should not automatically conclude that the disclosure is not permitted. Rather, the entity should review the Secretary's "exception determinations." If the state law at issue is not included among the determinations, then the entity may conclude that the disclosure is not permitted.[93]

Other HIPAA Provisions to Consider

This bulletin is primarily intended to highlight the provisions of the Privacy Rule that will permit covered entities to share PHI for public health purposes, but it is worthwhile to mention a few of the other sections of the Rule that covered entities should consider when using and disclosing PHI. This section serves only as a brief summary of relevant provisions and should by no means replace an entity's diligent review of the entire Rule.

Minimum Necessary

One of the overarching requirements of the Privacy Rule is that when a covered entity uses, discloses or requests PHI, it must "make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[94] The "minimum necessary" requirement imposes a significant responsibility on covered entities to establish appropriate policies and procedures for reviewing uses, disclosures and requests. The Rule establishes several exceptions to the requirement. Specifically, the requirement does not apply to:

- disclosures to or requests by a health care provider for treatment;
- uses or disclosures that are required by law;
- uses or disclosures made pursuant to a patient's written authorization;
- uses or disclosures made to the patient;

93. Exception determinations will be published in the Federal Register and will also be available on the DHHS Office for Civil Rights website (http://www.hhs.gov/ocr/hipaa). *See* 68 Fed. Reg. 11,554 (Mar. 11, 2003).

94. 45 C.F.R. § 164.502(b)(1); *see also* 45 C.F.R. § 164.514(d) (specific requirements applicable to the minimum necessary provision).

- disclosures made to the U.S. DHHS in accordance with the HIPAA regulations; and
- uses or disclosures that are required for compliance with the HIPAA regulations.[95]

Therefore, prior to disclosing PHI to a public health official or for a public health purpose, a covered entity should determine whether the minimum necessary requirement applies. For example, it will not apply when a provider:

- discloses PHI to a local health department so the department can provide treatment to a patient;
- reports a communicable disease to a local health department or reports child abuse or neglect to a local department of social services; or
- discloses PHI to a local health department or the state pursuant to the patient's written authorization.

The minimum necessary requirement will apply, for example, if the covered entity discloses PHI to a local health department for the department's payment or health care operations activities or to a pharmaceutical manufacturing company for the company's post-marketing surveillance of a new drug.

Verification Requirements

Verification of Identity and Authority

In most circumstances, the Privacy Rule requires covered entities to verify the *identity* of the person requesting PHI and that person's *authority* to have access to PHI.[96] Verification of identity and authority is not required if the covered entity already knows the person's identity and authority.[97]

With respect to disclosures for public health purposes, the practical implications of this requirement are that a covered entity must have policies and procedures in place for making such verifications and verify the identity and authority of any person requesting PHI if the entity does not already know the person's identity and authority.

In many instances, a request for information for public health purposes will come from a public official. The Privacy Rule identifies "safe harbors" for verifying the identity and authority of public officials.[98] For example, in order to verify a public official's identity, a covered entity may rely on an agency identification badge or a request on government letterhead. In order to verify the official's authority, a covered entity may rely on a written statement explaining the official's legal authority. A covered entity may always verify identity and authority by other means. These safe harbors for public officials are simply options available to the entity.

Verification of Documentation, Statements or Representations

The Privacy Rule requires covered entities to obtain documentation, statements, or representations from the person requesting the PHI before some disclosures can be made. For example, in order to disclose PHI for research purposes, a covered entity must obtain specific documentation from the researcher as to how the Rule's requirements for IRB or Privacy Board review were satisfied.[99] Such documentation also must be verified by the entity, but the Rule states that covered entities may rely on such materials that appear on their face to meet the applicable requirements.[100] A covered entity should review these verification provisions carefully to ensure that they are in compliance prior to disclosing PHI for public health purposes.

Notice of Privacy Practices

Most covered entities are required to provide patients with a "Notice of Privacy Practices."[101] The notice must include certain information, including a description of purposes for which the covered entity may use and disclose PHI.[102] A covered entity is

95. 45 C.F.R. § 164.502(b)(2).

96. 45 C.F.R. § 164.514(h); *see also* Jill Moore, "Verification Requirements" (May 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/verification.pdf.

97. Verification of identity is also not required in several other instances, including when disclosing PHI in disaster relief situations. 45 C.F.R. §164.514(h)(1)(i).

98. The Privacy Rule specifies that the entity may rely these "safe harbors" only if "such reliance is reasonable under the circumstances." 45 C.F.R. 164.514(h)(2)(ii)-(iii).

99. *See* 45 C.F.R. § 164.512(i)(2).

100. 45 C.F.R. § 164.514(h)(2)(i).

101. 45 C.F.R. § 164.520; *see also* Aimee Wall, "Right to a Notice of Privacy Practices" (Oct. 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/Upnotice.pdf (outline detailing the notice requirement).

102. 45 C.F.R. § 164.520(b)(ii)(B)-(C)

bound by its Notice. In other words, it may use and disclose PHI in a particular circumstance only if the Notice includes a description of that use or disclosure.[103] Therefore, it is critical that a covered entity anticipate the possible situations in which it may disclose PHI for public health purposes and describe those potential disclosures in the Notice. If the entity fails to include a description in its Notice that adequately addresses a specific public health disclosure and it is not legally *required* to make the disclosure by other law, then it is *prohibited* by the Privacy Rule from making the disclosure.

Accounting of Disclosures

The Privacy Rule generally requires covered entities to provide patients, upon request, with an accounting of most disclosures.[104] Certain types of disclosures discussed above may be excluded from the accounting, including disclosures

- to carry out treatment, payment and health care operations;
- pursuant to an authorization;
- disaster relief/notification;
- to correctional institutions; and
- as part of a limited data set.[105]

Unless the public health disclosure falls within one of the exceptions, a covered entity must have a system in place that allows it to produce an accounting of that public health disclosure when a patient submits a request.

Conclusion

In drafting the Privacy Rule, DHHS did "not intend to disturb or limit current public health activities."[106] In order to ensure that public health activities would be able to continue, it defined many different circumstances in which a covered entity is allowed to use or disclose PHI for public health purposes. Covered entities, however, must have a clear understanding of the requirements of the Privacy Rule and other applicable law and all of the limitations that apply to each type of use or disclosure *before* they use or disclose PHI.

103. 45 C.F.R. § 164.502(i).

104. 45 C.F.R. § 164.528; *see also* Aimee Wall, Right to an Accounting of Disclosures (Oct. 2002), *available at* http://www.medicalprivacy.unc.edu/pdfs/Upacctg.pdf (outline detailing the accounting requirements).

105. 45 C.F.R. § 164.528(a)(1).

106. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,917, 59,956 (Nov. 3, 1999).

This Bulletin is published by the Institute of Government to address issues of interest to local and state government employees and officials. Public officials may photocopy the Bulletin under the following conditions: (1) it is copied in its entirety; (2) it is copied solely for distribution to other public officials, employees, or staff members; and (3) copies are not sold or used for commercial purposes.

Additional copies of this Bulletin may be purchased from the Institute of Government. To place an order or to request a catalog of Institute of Government publications, please contact the Publications Sales Office, Institute of Government, CB# 3330 Knapp Building, UNC Chapel Hill, Chapel Hill, NC 27599-3330; telephone (919) 966-4119; fax (919) 962-2707; e-mail sales@iogmail.iog.unc.edu; or visit the Institute's web site at http://ncinfo.iog.unc.edu.

The Institute of Government of The University of North Carolina at Chapel Hill has printed a total of 247 copies of this public document at a cost of $220.90 or $.89 each. These figures include only the direct costs of reproduction. They do not include preparation, handling, or distribution costs.