Introduction

Public health officials in state and local health departments, as well as their partners in the health care system, have asked for clarification regarding the Privacy Rule and its impact on public health practice. The attached document, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)-- Privacy Rule: Provisions relevant to public health practice," contains excerpts from the website of the Office for Civil Rights (OCR) in the United States Department of Health and Human Services (http://www.hhs.gov/ocr/hipaa). Explanatory text from the OCR website is included, but the majority of the document consists of direct quotes from the Rule itself (with appropriate page references for the Federal Register). This compilation of excerpts highlights major provisions of the Rule that are relevant to public health practice.

Staff at the Centers for Disease Control and Prevention plan to work with the HHS Office for Civil Rights and other HHS agencies to put together guidance that addresses issues of relevance to public health. Such guidance will be posted on the OCR website listed above.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)-- Privacy Rule: Provisions relevant to public health practice

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the comments. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for 30 days. After that comment period, President Bush and Secretary Thompson decided to allow the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care.

Compliance Schedule
The final rule took effect on April 14, 2001. As required by HIPAA, most covered entities have two full years - until April 14, 2003 [or until April 14, 2004 for small health plans] - to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

Who must comply with these new privacy standards?
As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

What information is protected?
All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

For what disclosures and uses must consent be obtained by a provider?
The Privacy Rule states that:

> In general, "[a] covered health care provider [with a direct treatment relationship] must obtain the individual's consent,...prior to using or disclosing protected health information to carry out treatment, payment, or health care operations." (See section [§] 164.506, 65 Federal Register [F.R.] p. 82810, for complete requirements.)

What about sharing protected health information (PHI) with public health authorities?
The Privacy Rule allows for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public.

This practice is described in the preamble to the actual Rule:

> "The final rule continues to permit covered entities to disclose protected health information without individual authorization directly to public health authorities, such as the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention as well as state and local public health departments, for public health purposes as specified in the NPRM [Notice of Proposed Rulemaking for the Privacy Rule]." (65 F. R. p. 82526)

Which provision of the Privacy Rule addresses the sharing of PHI with public health authorities?
Sharing of PHI with public health authorities is addressed in §164.512, "Uses and disclosures for which consent, an authorization, or an opportunity to agree or object is not required." §164.512(a) permits disclosures that are required by law, which may be applicable to certain public health activities. **§164.512(b)** explicitly permits disclosures to public health authorities for public health activities:

> "(1) *Permitted disclosures*. A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph [§164.512(b)(1)] to:
>
> (i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;
> (ii) A public health authority... authorized by law to receive reports of child abuse or neglect;
>
> ...
>
> (iv) A person who may have been exposed to a communicable disease or may

> otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such a person as necessary in the conduct of a public health intervention or investigation; or..." (See §164.512(b)(1), 65 F. R. p. 82813-82814 for complete requirements.)

What if our agency acts both as a covered entity and a public health authority?
§164.512 (b) also answers this question regarding ***use*** of protected health information by a covered entity for public health purposes:

> "(2) *Permitted uses*. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section." (See §164.512(b)(2), 65 F. R. p. 82814 for complete requirements.)

The preamble to the Rule addresses this issue as well:

> "In addition, as in the NPRM, under the final rule, a covered entity that is acting as a public health authority–for example, a public hospital conducting infectious disease surveillance in its role as an arm of the public health department–may use protected health information in all cases for which it is allowed to disclose such information for public health activities as described above." (65 F. R. p. 82526)

How is a public health authority defined?

> *"Public health authority* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or 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, that is responsible for public health matters as part of its official mandate." (§164.501, 65 F. R. p. 82805)

The preamble to the Rule further describes the rationale behind the definition of public health authority:

> *"Public Health Authority...*
> In response to comments arguing that the provision is too broad, we note that section 1178(b) of the Act [Social Security Act], as explained in the NPRM, explicitly carves out protection for state public health laws. This provision states that: '[N]othing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.' In light of this broad Congressional mandate not to interfere with current public health practices, we believe the broad definition of 'public health authority' is appropriate to achieve that end." (65 F. R. pp. 82623-82624)

How much information may be used, requested, or shared?

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. (See §164.514(d) for specific requirements.)

Who determines what is the minimum necessary PHI for sharing with public health authorities?

Generally, the covered entity is responsible for determining the minimum amount of information reasonably needed to fulfill a request. In certain circumstances, however, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted, for example, when the request is made by a public official or agency for a disclosure permitted under §164.512 of the rule. §164.514(d) of the Rule describes this concept of reasonable reliance:

> "A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:
>
> > (A) Making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); ..." (See §164.514(d)(3)(iii), 65 F. R. p. 82819 for complete requirements)

What if a provider requests verification of the public health authority?

§164.514(h)(2) describes the verification requirements, including:

> "(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
>
> > (A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
> >
> > (B) If the request is in writing, the request is on the appropriate government letterhead; or
> >
> > (C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
>
> (iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority." (See §164.514(h), 65 F. R. p. 82820 for complete requirements.)

The preamble also addresses this issue:

"For most disclosures, verifying the authority for the request means taking reasonable steps to verify that the request is lawful under this regulation...Where the person requesting the protected health information is a public official, covered entities must verify the identity of the requester by examination of reasonable evidence, such as a written statement of identity on agency letterhead, an identification badge, or similar proof of official status. Similarly, covered entities are required to verify the legal authority supporting the request by examination of reasonable evidence, such as a written request provided on agency letterhead that describes the legal authority for requesting the release. Where §164.512 explicitly requires written evidence of legal process or other authority before a disclosure may be made [e.g., disclosures under §164.512(e), disclosures for judicial or administrative proceedings], a public official's proof of identity and the official's oral statement that the request is authorized by law are not sufficient to constitute the required reasonable evidence of legal authority; under these provisions, only the required written evidence will suffice.

In some circumstances, a person or entity acting on behalf of a government agency may make a request for disclosure of protected health information under these subsections. For example, public health agencies may contract with a nonprofit agency to collect and analyze certain data. In such cases, the covered entity is required to verify the requestor's identity and authority through examination of reasonable documentation that the requestor is acting on behalf of the government agency. Reasonable evidence includes a written request provided on agency letterhead that describes the legal authority for requesting the release and states that the person or entity is acting under the agency's authority, or other documentation, including a contract, a memorandum of understanding, or purchase order that confirms that the requestor is acting on behalf of the government agency." (65 F. R. p. 82547)

Will the Privacy Rule preserve existing, strong state confidentiality laws?

As required by the HIPAA law itself, state laws that provide greater privacy protection (which may be those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures

of health information, the final rule does not preempt these mandates.

What about other uses or disclosures for public responsibilities?
In limited circumstances, the final rule permits - but does not require - covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities.

These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security.

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

Sources (available at http://www.hhs.gov/ocr/hipaa/) :

U.S. Department of Health and Human Services. 45 CFR Parts 160 and 164. Standards for privacy of individually identifiable health information; final rule. Federal Register 2000;65:82462–82829.

Department of Health and Human Services Fact Sheet, "Protecting the Privacy of Patients' Health Information," July 6, 2001 (direct link available at http://www.hhs.gov/news/press/2001pres/01fsprivacy.html)

HHS's First Guidance for the Privacy Regulation, issued July 6, 2001