DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Director
Office for Civil Rights
200 Independence Ave., SW Rm 509F
Washington, DC 20201

September 9, 2005

U.S. Department of Health and Human Services Office for Civil Rights

HURRICANE KATRINA BULLETIN #2:

HIPAA Privacy Rule Compliance Guidance and Enforcement Statement For Activities in Response to Hurricane Katrina

Background

Hundreds of thousands of evacuees from areas affected by Hurricane Katrina have been relocated to shelters across the country. For many, an important need is to identify and provide prescription medications. However, medical and prescription records of many evacuees either are lost or inaccessible.

Health plans and health care providers are working together with other industry segments to gather and provide this information to the appropriate points of care for the evacuees. The information below provides guidance on how the HIPAA Privacy Rule applies to these activities, as well as describes the HHS Office for Civil Rights' enforcement approach in light of these emergency circumstances.

Compliance Guidance

The ***Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations*** (attached), issued by OCR, emphasizes the broad range of permissible disclosures that covered entities may make to respond to the needs of evacuees in these situations. For example, health plans and health care providers may disclose prescription and other health information to health care providers at shelters to facilitate treatment of the evacuees.

In addition, business associates that are managing such information on behalf of covered entities may make these disclosures to the extent permitted by their business associate agreements with the covered entities, as provided in the Privacy Rule. For example, a business associate agreement may broadly permit the business associate to make disclosures the covered entity is permitted to make, or may otherwise permit the business associate to make treatment or other disclosures as permitted by the Privacy Rule. If the business associate agreement does not permit such disclosures, the covered entity and business associate can amend the agreement to permit them.

Similarly, if a business associate uses an agent to assist in performing its business associate functions, the business associate must ensure that the agent agrees to the privacy restrictions and conditions that apply to the business associate. The agreement between a business associate and its agent may also broadly permit the agent to make disclosures the covered entity is permitted to make or may otherwise permit the agent to make treatment or other disclosures permitted by the Privacy Rule.

Covered entities or their business associates may provide health information on evacuees to another party for that party to manage the health information and share it as needed for providing health care to the evacuees. Where a covered entity provides protected health information to another for this purpose, the Privacy Rule requires the covered entity to enter into a business associate agreement with this party. If the business associate, rather than the covered entity itself, is providing this information to another party that is acting as its agent, the covered entity's business associate must enter into an agreement to protect health information with this party. See 45 CFR 164.504(e)(2)(ii)(D).[1]

Enforcement Approach

Under section 1176(b) of the Social Security Act, HHS may not impose a civil money penalty where the failure to comply is based on reasonable cause and is not due to willful neglect, and the failure to comply is cured within a 30-day period. HHS has the authority to extend the period within which a covered entity may cure the noncompliance "based on the nature and extent of the failure to comply." We advise that in determining whether reasonable cause exists for a covered entity's failure to meet the business associate requirements and in determining whether and to what extent to extend the period within which noncompliance must be cured, OCR will consider the emergency circumstances arising from Hurricane Katrina, along with good faith efforts by covered entities, its business associates and their agents, both to protect the privacy of health information and to appropriately execute the agreements required by the Privacy Rule as soon as practicable.

Further, OCR advises that, in the exercise of its enforcement discretion, where a complaint is filed arising from uses and disclosures of protected health information by a covered entity, its business associate or agent of a business associate, that would have been permissible had there been a business associate agreement as required by the Rule, OCR will not take enforcement action or seek to impose civil money penalties where, due to the urgency of the circumstances arising from Hurricane Katrina, a covered entity, its business associates or their agents, are unable to formalize such agreements as required by the Rule in sufficient time to meet the immediate needs of the evacuees, but appropriately execute the required agreements as soon as practicable.

[1] Sample business associate agreement provisions are attached and also available at http://www.hhs.gov/ocr/hipaa/. These sample provisions may be modified as necessary to meet the limited purposes of this emergency situation and particular business contexts, consistent with the requirements of 45 CFR 164.502(e) and 164.504(e) of the Privacy Rule.

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Director
Office for Civil Rights
200 Independence Ave., SW Rm 509F
Washington, DC 20201

September 2, 2005

U.S. Department of Health and Human Services Office for Civil Rights

HURRICANE KATRINA BULLETIN: HIPAA PRIVACY and DISCLOSURES IN EMERGENCY SITUATIONS

Persons who are displaced and in need of health care as a result of a severe disaster – such as Hurricane Katrina – need ready access to health care and the means of contacting family and caregivers. We provide this bulletin to emphasize how the HIPAA Privacy Rule allows patient information to be shared to assist in disaster relief efforts, and to assist patients in receiving the care they need.

Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all the following ways:

- ✓ **TREATMENT.** ***Health care providers can share patient information as necessary to provide treatment***.
  - *Treatment* includes
    - sharing information with other providers (including hospitals and clinics),
    - referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
    - coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).
  - Providers can also share patient information to the extent necessary to seek payment for these health care services.
- ✓ **NOTIFICATION.** ***Health care providers can share patient information as necessary to identify, locate and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.***
  - The health care provider should get verbal permission from individuals, when possible; but, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
    - Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify or otherwise

notify family members and others as to the location and general condition of their loved ones.

- In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

- ✓ **IMMINENT DANGER.** Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider's standards of ethical conduct.

- ✓ **FACILITY DIRECTORY**. Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

ATTACHMENT 2

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions[1]

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].

b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.
g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
f. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]
g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
j. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate
General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:

   Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
   [List Purposes].

b. Refer to underlying services agreement:

   Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business

Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).
d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]
b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
    1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections

____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.
    1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
    2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

[1] *Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.*