DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, Maryland 21244-1850

CENTERS for MEDICARE & MEDICAID SERVICES

Center for Medicaid and State Operations

Ref: S&C-03-15

DATE: **March14, 2003**

FROM: Director
Survey and Certification Group

SUBJECT: Review of Protected Health Information and Applicability of Business Associate Agreements Under the Health Insurance Portability and Accountability Act (HIPAA) for the Purposes of Survey and Certification

TO: Survey and Certification Regional Office Management (G-5)
State Survey Agency Directors

The purpose of this letter is to provide guidance regarding the appropriateness of executing business associate agreements between the state survey agencies (SAs) and providers, and the provision of individually identifiable health care information during surveys under the HIPAA Privacy Rule. Several SAs have received requests from providers to enter into business associate agreements, which were addressed in the "Standards for Privacy of Individually Identifiable Health Information" (HIPAA Privacy Rule) published December 28, 2000, and most recently amended August 14, 2002 (65 Fed. Reg. 82462, as modified by 67 Fed. Reg. 53182). Additionally, several providers have expressed concern over the release of protected health information (PHI) to surveyors under the HIPAA Privacy Rule.

The Administrative Simplification provisions of HIPAA apply to health plans, health care clearinghouses, and health care providers that transmit individually identifiable health information in electronic form.

While the HIPAA Privacy Rule provides for certain privacy rights for the subjects of PHI, those rights have limitations. For example, the HIPAA Privacy Rule provides that PHI may be used and disclosed without the authorization of the subject of that information to the extent a law requires the production of that information. *(See 45 CFR 164.512(a)).* The HIPAA Privacy Rule also provides that PHI may be used and disclosed without the authorization of the subject of that information for health oversight activities that are authorized by law. Examples are inspection, licensure and other activities necessary for the appropriate oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards. *(See 45 CFR 164.512(d)).*

To the extent that the information sought is PHI for survey and certification work that is responsive to a law that requires the production of that information, or to the extent the information sought is for health oversight activities authorized by law, the surveyed entity does not need to receive an authorization prior to releasing the necessary PHI to the SA under the HIPAA Privacy Rule.

Government regulatory programs that function as health oversight agencies that need PHI to determine a facility's compliance with program standards do not need to obtain an individual's authorization to use that individual's health records for the appropriate oversight of entities subject to that program's regulation. The health oversight agency must limit its uses and disclosures of this PHI to the minimum necessary to accomplish the program's regulatory purpose, and it may not use records obtained under this exception to investigate the individual whose records they have obtained. Disclosures made pursuant to a law that mandates the production of information are not subject to any limitations under the HIPAA Privacy Rule so long as the disclosure complies with and is limited to the relevant requirements of such law.

In summary, to the extent that the information sought by an SA is PHI for survey and certification work that is either 1) required by law or 2) for health care oversight activities, the surveyed entity does not need to receive an authorization prior to releasing the necessary PHI to the SA. Furthermore, surveyed entities do not need to execute a business associate agreement with SAs prior to releasing PHI as SAs are not business associates of the surveyed entities under the HIPAA Privacy Rule definition of "business associate." SAs do not conduct a function or activity of the surveyed entity on the surveyed entity's behalf. (*See 45 CFR 160.103).*

We have attached a suggested template for use by the SAs in response to requests to take part in business associate agreements with providers, and to address provider's concerns over the release of PHI for oversight activities.

Effective Date: April 14, 2003

Training: The information contained in this announcement should be shared with all survey and certification staff, their managers and the state/RO training coordinator.

/s/
Steven A. Pelovitz

Attachment

Mr. (Mrs., Ms.) X
Administrator
Facility Name
Street Address
City, State Zip Code

Re: Release of Patient Information for Survey and Certification Activities

Dear :

The purpose of this letter is to address your concerns about the release of protected health information (PHI) for the purpose of survey and certification activities.

The Standards for Privacy of Individually Identifiable Health Information, otherwise known as the Health Insurance Portability and Accountability Act or "HIPAA Privacy Rule" *(45 CFR Parts 160 and 164)* guarantee certain privacy rights to individuals. The HIPAA Privacy Rule provides that PHI may be used and disclosed without the authorization of the subject of that information to the extent a law requires the production of that information. (*See 45 CFR 164.512(a)*). The HIPAA Privacy Rule also provides that PHI may be used and disclosed to Health Oversight Agencies without the authorization of the subject of that information for health oversight activities that are authorized by law. Examples are inspection, licensure and other activities necessary for the appropriate oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards. *(See 45 CFR 164.512(d)).*

As such, an individual's authorization is not required for information supplied to government regulatory programs that qualify as health oversight agencies needing PHI to determine compliance with program standards as part of that oversight agency's appropriate oversight of entities subject to that program's regulation. A Health Oversight Agency (like those that conduct survey and certification activities) must limit its uses and disclosures of PHI to the minimum necessary to accomplish the program's regulatory purpose, and may not use records obtained under this exception to investigate the individual patient whose records they have obtained. Disclosures made pursuant to a law that mandates the production of information are not subject to any limitations under the HIPAA Privacy Rule so long as the disclosure complies with and is limited to the relevant requirements of that law.

To the extent that the information sought for survey and certification work is responsive to a law that requires the production of that information, or to the extent the information sought by a health oversight agency for health oversight activities authorized by law, the surveyed entity does not need an authorization prior to releasing the necessary PHI to the SAs. Nor do surveyed entities need to execute a business associate agreement with the SAs prior to releasing PHI as SAs are not business associates of the surveyed entities under the HIPAA Privacy Rule definition of "business associate."

If you have any further questions or comments on this matter, please contact NAME at NUMBER or ADDRESS

Signature
Printed Name