STATE OF COLORADO

Bill Owens, Governor
Douglas H. Benevento, Executive Director

Dedicated to protecting and improving the health and environment of the people of Colorado

4300 Cherry Creek Dr. S.
Denver, Colorado 80246-1530
Phone (303) 692-2000
TDD Line (303) 691-7700
Located in Glendale, Colorado

http://www.cdphe.state.co.us

Laboratory Services Division
8100 Lowry Blvd.
Denver, Colorado 80230-6928
(303) 692-3090

Colorado Department
of Public Health
and Environment

April 24, 2003

# HIPAA
# HFD Surveyor Information Kit

Table of Contents

**FACTS ABOUT THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA")**
**SPRING 2003**

## I. Our Role

HIPAA is a law that was passed in 1996, with various requirements and implementation dates. The biggest pieces of HIPAA become effective this year. HIPAA governs the manner in which a person's private or protected health information can be used. Generally, covered entities (healthcare providers) must protect and keep confidential the health information of individuals. There are, however, exceptions, for example disclosure authorizations are NOT required for the use of individual's health information when used for treatment, payment and healthcare operational (TPO). HFD does not fall in the TPO category, but covered entities and their business associates do. Disclosures made to the person, or made with the person's authorization, or for TPO purposes DO NOT need to be tracked; however, public health disclosures and other permissable disclosures such as to health oversight agencies DO need to be tracked.

HIPAA applies to any entity that handles private health information, such as a health plan, billing company, health care facility, etc. (covered entities). This means it applies equally to facilities that are certified and those that are only state licensed.

HIPAA also applies to entities that are considered "business associates" of a covered entity. A business associate is defined as an agent, contractor, or other hired to do work on behalf of a covered entity that requires access to and use of private health information. Some of our facilities mistakenly believe HFD is a business associate of theirs, but as a government agency responsible for regulatory and health oversight, we are NOT a business associate of anyone, including Medicare (CMS) and Medicaid (HCPF).

HFD is also NOT responsible for determining through surveys or investigations if covered entities are HIPAA compliant; nor are HFD staff-members advisors or resources for facilities that have HIPAA questions or are trying to become HIPAA compliant. Providers should address these types of HIPAA compliance questions to their attorneys or other qualified HIPAA consultants.

## II. Disclosure

The HIPAA privacy requirement is effective as of April 14, 2003. After this date, covered entities are required to track and account for disclosures of individually identifiable health information, sometimes referred to as protected health information (PHI). This includes disclosures to health oversight agencies (HOA) such as HFD.

How does this affect HFD survey work? As an HOA, HFD doesn't need an individual's prior permission to use or look at PHI, but we do have to limit our use and disclosure to the minimum information necessary to accomplish our regulatory purpose.

At the request of many Colorado healthcare providers, HFD has developed a "HIPAA Disclosure Protocol" to clarify and address how covered entities and HFD can work together in an efficient and accurate way to meet our individual HIPAA requirements during surveys, investigations and other

regulatory or HOA events. Surveyors and investigators must follow this protocol to ensure that the HIPAA privacy rules are followed and that covered entities receive the necessary PHI accounting to comply with the privacy rule. Briefly, the HFD HIPAA Disclosure Protocol includes four steps:

1. Surveyors and investigators will hand deliver a "HIPAA Release of Patient Information for Health Oversight Agency Certification and Licensure Events and Activities" letter to covered entities at entry or start of a survey, investigation, or other regulatory or HOA activity or event. This letter states that HOAs are not business associates of covered entities and that individuals' PHI may be used and disclosed to the HOA without prior authorization of the individuals;
2. Surveyors and investigators will keep accurate records of the start and end dates of the regulatory and HOA event and whose PHI was used and disclosed (in most cases this will be the survey sample list);
3. When written findings are sent to the covered entity at the end of the regulatory or HOA event (e.g., survey results, investigative findings, CMS 2567) a written accounting of PHI disclosures will also be provided to the covered entity by HFD. This disclosure will include a brief statement of the purpose of the disclosure, a brief summary of information disclosed, dates of disclosure and whose PHI was disclosed (sample list);
4. The covered entity may use the disclosure documents from this protocol to account for the PHI disclosure after the regulatory or HOA event is concluded.

## III. Dates

**April 14, 2003** – The deadline for compliance with the privacy requirements.
**April 16, 2003** – For those who submitted a "compliance extension plan" and received a one-year extension for complying with the electronic transaction and code set standards, you should start testing your software no later than (or make sure your third party billers/clearinghouses do so) this date to ensure you will be able to move the health care data in the new standardized format.
**October 16, 2003** – The deadline for complying with the electronic transaction and code set standards required for those who requested an extension.

## IV. Enforcement

As of April 14, 2003, enforcement will be shared between the Office of Civil Rights ("OCR") in the U.S. Department of Health and Human Services and CMS. OCR will be responsible for enforcing the privacy standards; CMS will be responsible for enforcing the transaction standards. CMS believes the process leading to an enforcement action will likely be in response to an external complaint filed against a covered entity. While there is a rumor that a new federal HIPAA enforcement tag is coming out, this has not been confirmed and no particulars are known. As of now, there is no F tag associated with HIPAA, but there is a requirement under F516 to keep all patient or resident records confidential.

## V. Resources

HFD surveyors and staff – if you have questions or need assistance with HIPAA issues contact:

| | | |
|---|---|---|
| John Schlue | John.Schlue@state.co.us | 303-692-2817 or |
| Melissa Barkett-Long | Melissa.Barkett@state.co.us | 303-692-2927 |

Covered Entities and HFD surveyors and staff – you can get information on HIPAA at:

- Sign up for free email listserv at http://aspe.os.dhhs.gov/admnsimp/lsnotify.htm
- Internet web site www.cms.hhs.gov/hipaa
- Email HIPAA questions to askhipaa@cms.hhs.gov
- Phone HIPAA questions to 1-866-282-0659 or 1-866-627-7748
- Office of Civil Rights www.hhs.gov/ocr/hipaa
- State of Colorado http://www.state.co.us/gov_dir/govnr_dir/ospb/hipaa/index.html

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


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

STATE OF COLORADO

Bill Owens, Governor
Douglas H. Benevento, Executive Director

Dedicated to protecting and improving the health and environment of the people of Colorado

4300 Cherry Creek Dr. S.
Denver, Colorado 80246-1530
Phone (303) 692-2000
TDD Line (303) 691-7700
Located in Glendale, Colorado

http://www.cdphe.state.co.us

Laboratory Services Division
8100 Lowry Blvd.
Denver, Colorado 80230-6928
(303) 692-3090

Colorado Department
of Public Health
and Environment

April 14, 2003

Administrator
Colorado Healthcare Facility or Agency – HIPAA Covered Entity

Re: Release of Patient Information for Health Oversight Agency Certification and Licensure Events and Activities

Dear Administrator:

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

Administrator
HIPAA Release of Patient Information
April 14, 2003

To the extent that the information sought for certification and licensure 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 HOA. Nor do surveyed entities need to execute a business associate agreement with the HOA prior to releasing PHI as HOAs are not business associates of the surveyed entities under the HIPAA Privacy Rule definition of "business associate."

Health Facilities Division has developed the following "HIPAA Disclosure Protocol" to assist covered entities with accounting for the disclosure of PHI during health oversight agency events.

1. Surveyors and investigators will provide covered entities with this "HIPAA Release of Patient Information for Health Oversight Agency Certification and Licensure Events and Activities" letter at entry or start of a survey, investigation, or other regulatory or HOA activity.
2. Surveyors and investigators will keep accurate records of the start and end dates of the regulatory or HOA event and whose PHI was used and disclosed (in most cases this will be the survey sample list);
3. When written findings are sent to the covered entity at the end of the regulatory or HOA event (e.g., survey results, investigative findings, CMS 2567), a written accounting of PHI disclosures will also be provided to the covered entity by Health Facilities Division. This disclosure will include a brief statement of the purpose of the disclosure, a brief summary of information disclosed, dates of disclosure and whose PHI was disclosed (sample list);
4. The covered entity may use the disclosure documents from this protocol to account for the PHI disclosure after the regulatory or HOA event is concluded.

For information on HIPAA:

- Sign up for free email listserv at http://aspe.os.dhhs.gov/admnsimp/lsnotify.htm
- Internet web site www.cms.hhs.gov/hipaa
- Email HIPAA questions to askhipaa@cms.hhs.gov
- Phone HIPAA questions to 1-866-282-0659 or 1-866-627-7748

If you have any questions or comments about the HFD disclosure protocol, please contact:

| | | |
|---|---|---|
| John Schlue | john.schlue@state.co.us | 303-692-2817 or |
| Melissa Barkett-Long | melissa.barkett@state.co.us | 303-692-2927 |

Sincerely,

Health Facilities Division

STATE OF COLORADO

Bill Owens, Governor
Douglas H. Benevento, Executive Director

Dedicated to protecting and improving the health and environment of the people of Colorado

4300 Cherry Creek Dr. S.
Denver, Colorado 80246-1530
Phone (303) 692-2000
TDD Line (303) 691-7700
Located in Glendale, Colorado

http://www.cdphe.state.co.us

Laboratory Services Division
8100 Lowry Blvd.
Denver, Colorado 80230-6928
(303) 692-3090

Colorado Department
of Public Health
and Environment

Date

Mr. (Mrs., Ms.) X, Administrator
Facility Name

Re: HIPAA Disclosure of Protected Health Information During Regulatory or Health Oversight Agency Event

The HIPAA Privacy Rule provides that protected health information (PHI) may be used and disclosed without authorization of the subject of that information to the extent a law requires production of that information (45 CFR 164.512(a)). The privacy rule also provides that PHI may be used and disclosed without the authorization of the subject of that information for health oversight activities (HOA) that are authorized by law, e.g., surveys, inspections, licensure, other regulatory oversight activities (45 CFR 164.512(d)).

This HIPAA disclosure letter provides you with information about a recent event in which Health Facilities Division staff used or looked at the PHI of individual(s) in your care.

**Purpose of Disclosure**

- ❑ Standard survey for certified or licensed program.
- ❑ Complaint or occurrence investigation for certified or licensed program.
- ❑ Hospital EMTALA or complaint investigation.
- ❑ Survey revisits.

**Information Disclosed**

- ❑ During this regulatory or health oversight event the following PHI was or may have been used or looked at by Health Facilities Division staff: individual(s) medical or personal records; interviews with individual(s), family members, covered entity staff or other outside parties such as clergy, volunteers, Ombudsmen, physicians, clinicians, etc. about the individual(s) care, medical and mental condition and their daily living conditions and activities.

**Dates of Disclosure**

- ❑ Dates of disclosure for this regulatory or HOA event:
  Start _____ End _____.

**Individual(s) whose PHI was Disclosed**

See enclosed **sample list** of individual(s) names.

*Note: Sample lists for onsite and documentation revisits, where the resident/patient sample list from the original regulatory or HOA event has not changed, will not be enclosed with the revisit HIPAA disclosure letter. For these circumstances the covered entity should use the original event's sample list for this disclosure. A new revisit sample list will be enclosed only when new citations are made or new or different resident/patients are part of the revisit sample.*

Sincerely,
Health Facilities Division