Notice of Proposed Rule
HIPAA Privacy Rule on Accounting of Disclosures and Access Reports

The U.S. Department of Health and Human Services has issued a Notice of Proposed Rule to modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The purpose of the modifications is, in part, to implement the statutory requirement under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") to require covered entities and business associates to account for disclosures of protected health information (PHI) to carry out treatment, payment and health care operations if such disclosures are through an electronic record. Pursuant to both the HITECH Act and its more general authority under HIPAA, HHS, is proposing to expand the requirement to Account for Disclosures of PHI.

HHS is proposing to revise Section 164.528 of the HIPAA Privacy Rule by dividing it into two separate rights for individuals: paragraph (a) would set forth an individual's right to an accounting of disclosures and paragraph (b) would set forth an individual's right to an Access Report (which would include electronic access by both workforce members and persons outside of the covered entity).

These two rights, to an Accounting of Disclosures and to an Access Report, would be distinct but complementary. The right to an Access Report would provide information on who has accessed electronic protected health information in a designated record set (including for purposes of treatment, payment and health care operations), while the right to an Accounting of Disclosures would provide additional information about the disclosure of designated record set information (whether hard copy or electronic) to persons outside the covered entity and its business associate for certain purposes (e.g. law enforcement, judicial hearings, public health investigations). The intent of the Access Report is to allow individuals to learn if specific persons have accessed their electronic designated record set information (it will not provide information about the purposes of the person's access.) In contrast, the intent of the Accounting of Disclosures is to provide more detailed information for certain types of disclosures.

The term "designated record set" include the medical and health payment records maintained by or for a covered entity used by or for the covered entity to make decisions about individuals.

Most medical practices are "covered entities" under HIPAA and will be substantially affected by the proposed regulation. There is concern that the proposed regulations would impose new onerous requirements on physician practices that would be difficult to achieve. For more information see the summary "PROPOSED HIPAA PRIVACY RULE ON ACCOUNTING OF DISCLOSURES AND ACCESS REPORTS".

SUMMARY: PROPOSED HIPAA PRIVACY RULE ON ACCOUNTING OF DISCLOSURES AND ACCESS REPORTS

The U.S. Department of Health and Human Services has issued proposed regulations that would modify the HIPAA standard for Accounting of Disclosures of Protected Health Information. Pursuant to the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and its' more broad authority under HIPAA, HHS is proposing to expand the accounting provision to provide individuals with the right to receive an Access Report indicating who has accessed electronic protected health information in a designated record set. HHS is also proposing to expand the Accounting of Disclosures requirement.

The public may submit comments to HHS on or before August 1, 2011.

Comments may be submitted via Federal Rulemaking Portal:http://www.regulations.gov. or Regular, Express or Overnight mail to:

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HIPAA Privacy Rule Accounting of Disclosures
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington D.C. 20201

Submit one original and two copies.

Current Requirement Under HIPAA

HIPAA at 42 CFR164.528 requires covered entities to make available to an individual upon request accounting of certain disclosures of an individual's Protected Health Information (PHI) made during the six year period prior to the request. The accounting requirement applies to PHI in both electronic and hard copy.

A "disclosure" is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information".

For each disclosure, the accounting must include:

(1) The date of the disclosure;
(2) The name (and address, if known) of the entity or person who received the PHI;
(3) A brief description of the information disclosed; and
(4) A brief statement of the purpose of the disclosure.

For multiple disclosures to the same person for the same purpose, the accounting is only required to include: (1) For the first disclosure, a full accounting, with the

elements described above; (2) the frequency, periodicity, or number of disclosures made during the accounting period; and (3) the date of the last such disclosure during the accounting period.

Section 164.528(a)(i) provides that an accounting must include all disclosures of PHI, except for disclosures:

- To carry out treatment, payment and health care operations, 164.506;
- To individuals of PHI about them as provided in 164.502
- Incident to a use or disclosure otherwise permitted or required, as provided in 164.502;
- Pursuant to an authorization, 164.508;
- For the facility's directory or to persons involved in the individual's care or other notification purposes, 164.510;
- For national security or intelligence purposes, 164.512(k)(2);
- To correctional institutions or law enforcement officials, 164.512(k)(5);
- As part of a limited data set in accordance with 164.514(e); or
- That occurred prior to the compliance date for the covered entity.

For disclosures for research in accordance with 164.512(i) (such as disclosures subject to an Institutional Review Board's waiver authorization) involving 50 or more individuals, 164.528(b)(4) permits the covered entity to provide a list of research protocols rather than specific information about each disclosure.

Changes Required by the HITECH Act

The HITECH Act provides that the exemption for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures "through an electronic health record". Section 13400 of the HITECH Act defines an EHR as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff". Under Section 13405(c), an individual has a right to receive an accounting of such disclosures made during the three year period prior to the request. With respect to disclosures by business associates through an EHR to carry out treatment, payment, and health care operations on behalf of a covered entity, Section 13405(c) requires the covered entity to provide either an accounting of the business associates' disclosures, or a list and contact information of all business associates in order to enable the individual to contact each business associate for an accounting of the business associate's disclosures. A business associate includes any person (other than a member of the covered entity's own workforce) such as a contractor, vendor, outsourced provider or other business, that provides a service to the covered entity and must have access to the covered entity's PHI in order to provide such service. Although a business associate is not considered to be a "covered entity" under the HIPAA Privacy Rule, the HIPAA Privacy Rule still applies to the PHI in the care of a business associate. Covered entities are required to establish "business associate agreements" or contracts to safeguard the privacy of PHI with their business associates. An example of a business associate is an attorney who may require a physician's PHI in

order to provide legal services to the physician. Another example is a medical society, which may require a physician's PHI in order to advocate on behalf of the physician.

On May 3, 2010 HHS published a request for information (RFI) seeking information on individuals' interests in learning of disclosures, the burdens on covered entities in accounting for disclosures, and the capabilities of technology. HHS received approximately 170 comments. The majority of comments were from covered entities. Most of the covered entities (over 80) stated that providing an accounting of treatment, payment and health care operations disclosures would provide little to no benefit to individuals. Most covered entities responded that since the Privacy Rule's compliance date in 2003, they have received no or very few requests for accounting of disclosures. A large percentage of the comments expressed concerns that the new accounting of disclosure requirements would create increased costs, reduce patient care time resulting in disruptions in provider workflow, and a potential chilling effect on the adoption of EHR systems, particularly for small providers. Notwithstanding, HHS is proposing to expand the Account of Disclosures requirements.

HHS is proposing to divide the rights of individuals into two separate rights (a) an individual's right to an Accounting of Disclosures; and (b) an individuals' right to an Access Report. The Access Report would include electronic access by both workforce members of the covered entity and persons outside the covered entity.

These two rights, to an Accounting of Disclosures, and to an Access Report, would be distinct but complementary. The right to an Access Report would provide information on who has accessed electronic PHI in a designated record set (including access for purposes of treatment, payment, and health care operations), while the right to an Accounting Disclosures would provide additional information about disclosures of designated record set information whether hard-copy or electronic to persons outside the covered entity and its business associates for certain purposes. The intent of the Access Report is to allow individuals to learn if specific persons have accessed their electronic designated record set information (it will not provide information about the purposes of the person's access). In contrast, the intent of the Accounting of Disclosures is to provide more detailed information for certain types of disclosures.

The right to an Access Report would only apply to PHI about an individual that is maintained in an electronic data record set. The proposed rule would provide an individual with a right to obtain an "Access Report". It would cover a three year period, and would provide the individual with information about who has accessed the individual's electronic PHI held by a covered entity or a business associate. It would not distinguish between "uses" and "disclosures", and thus would apply when any person accesses an electronic designated record set, whether the person is a member of the workforce of the covered entity or a person outside of the covered entity. Under the proposed rule, the Access Report must identify the date, time, and name of the person (or name of the entity if the person's name is unavailable) who accessed the information. HHS is also proposing to require inclusion of a description of the PHI that was accessed and the user's action, but only to the extent that such information is available.

Business Associates - With respect to the individual's right to an accounting of disclosures and the right to an Access Report, covered entities would be required to include the applicable uses and disclosures of their business associates. This means if the business associate has PHI in a designated record set, the business associate will be required to keep track of disclosures in order to comply with the Accounting of Disclosures requirement. If the business associate has electronic PHI in a designated record set, the business associate would be required to comply with the Access Report requirement. If the business associate does not have designated record set PHI, the business associate would not be affected.

HHS is proposing that covered entities and business associates provide individuals with a right to an Access Report beginning January 1, 2013 for electronic designated record systems acquired after January 1, 2009. HHS is proposing that covered entities and business associates provide individuals with a right to an Access Report beginning January 1, 2014, for electronic designated record set systems acquired as of January 1, 2009.

Definition of "designated record set" – Designated record sets include medical and health care payment records maintained by or for a covered entity, and other records used by or for the covered entity to make decisions about individuals.

Examples of PHI that fall outside of designated record set:

Peer review records – these files are used to improve patient care but are not used to make decisions about the individual.

A. **Accounting for Disclosures – Section 164.528(a)**

1. HHS proposes to change the scope of information subject to the accounting to the information about an individual in a designated record set, to explicitly include business associates in the language of the standard, and to shorten the accounting period from 6 years to 3. Currently, 164.528 lists the types of disclosures that are exempt from the accounting. Instead, HHS proposes to modify the regulation to list the types of disclosures that are subject to the accounting.

Currently an individual has a right to an accounting of PHI regardless of where such information is located. HHS is proposing to limit the accounting requirement to PHI about the individual in a designated record set.

Covered entities and business associates should have documentation to track the PHI that are part of a designated record set.

PHI outside the designated record set would not be subject to the accounting requirement but would otherwise remain protected under the HIPAA Privacy Rule.

HHS is requesting comment on its proposal to limit the accounting requirement of PHI in a designated record set as opposed to all PHI.

2. **What type of Disclosure will be subject to Accounting?**

HHS is proposing to explicitly list the types of disclosure that are subject to the accounting requirement (rather than the current approach which lists the exceptions to the accounting requirement).

CMS Proposes:

- To continue to require accounting for disclosures that are impermissible under the Privacy Rule. This will include impermissible disclosures that did not rise to the level of breach (e.q. because the disclosure did not compromise the security or privacy of the PHI) that was subject to the Breach Notification Rule – see 164.404.
- HHS is proposing to exempt from accounting impermissible disclosures that were subject to the Breach Notice Rule (since notice was already provided.)
- HHS is proposing to continue to include the accounting requirement for disclosures for public health activities (except those involving reports of child abuse or neglect), for judicial and administrative proceedings, for law enforcement activities, to avert a serious threat to health or safety, for military and veteran activities, for the Department of State's medical suitability determinations, and to government programs providing public benefits, and for workers' compensation.
- HHS is proposing to exempt from accounting reports of child abuse or neglect to a public health authority or other appropriate government authority (HHS finally realizes that harm can result to the covered entity if this type of disclosure is subject to accounting).
- HHS is proposing to continue to exclude the following types of disclosure from the account requirement: (i) to individuals who are the subject of the PHI, 164.502; (ii) incident to a use or disclosure otherwise permitted or required by the Privacy Rule, 164.502; (iii) pursuant to an Authorization, 164.508; (iv) for the facility's directory or to persons involved in the individual's care or other notification purposes as provided in 164.510; (v) for national security or intelligence purposes, 164.512(k)(2); (vii) as part of a limited data set in accordance with 164.514(e); or (viii) disclosure that occurred prior to the compliance date for the covered entity.
- Disclosures for treatment, payment and health care operations would continue to be exempt for paper records. However, in accordance with Section 13405(c) of HITECH, an individual would be able to obtain information (such as the name of the person accessing the information) for all access to electronic PHI stored in a designated record set for purposes of treatment, payment or health care operations.
- HHS is proposing to exempt from accounting requirements certain categories of disclosures that are currently subject to accounting: victims of abuse, neglect or

domestic violence 164.512(c); disclosures for health oversight activities, 164.512(d); disclosures for research purposes, 164.512(i); disclosures about decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation 164.512(g) and (h); disclosures for protective services for the President and others, 164.512(k)(3); and most disclosures required by law.

3. **Content of the Accounting**

Currently the Privacy Rule at 164.528(b)(2) requires an accounting of disclosures to include date of disclosure, name and (if known) address of the recipient, a brief description of the type of PHI disclosed, and a brief statement of the purpose of the disclosure. HHS is proposing to maintain these elements with some minor modifications.

Although individuals would have a right to an accounting of all included disclosures occurring within the 3 year period prior to the request, HHS is proposing that the covered entity be required to provide individuals the option of limiting the accounting to a particular time period, type of disclosure or recipient.

4. **Provision of Accounting**

a) HHS is proposing to reduce the response time for an accounting from 60 days to 30 days. HHS is proposing a single 30 day extension if it will take more than 30 days to respond.

HHS is requesting comments whether shortening the response time may unreasonably burden covered entities. HHS is requesting comments regarding how long it takes to collect information necessary for an accounting, including collecting the necessary information from business associates, and to generate an accounting of disclosures.

b) HHS is proposing to require the covered entity to provide the accounting in the form (e.g. paper or electronic) and format (e.g. compatibility with a specific software application) requested by the individual. If an individual requests a particular form such as a PDF file, the covered entity will be required to provide the accounting in that format if readily producible.

c) HHS proposes to clarify that a covered entity may require individuals to make a request for an accounting in writing.

d) HHS proposes to continue to provide that a covered entity may not charge for the first request for an accounting in a 12-month period, but may charge a reasonable cost-based fee for providing an accounting in response to subsequent requests in the 12-month period. HHS proposes that the covered entity would be required to inform the individual at the time of the first request that all subsequent requests in the 12-month period may be subject to a fee.

5. **Documentation**

The current rule requires that covered entities must document and retain the information necessary to generate an accounting of disclosures, a copy of the written accounting that is provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting.

Accordingly, under the current Rule, a covered entity must maintain for 6 years the information necessary to generate an accounting of disclosures.

HHS is proposing to reduce the accounting period from 6 years to 3 years. HHS is, therefore, proposing that a covered entity must document and retain the information necessary to generate an accounting of disclosures for 3 years-rather than the current 6 years required, see 164.530(j).

B. **Right to an Access Report-Section 164.528(b)**

In addition to the right to an accounting of disclosures under Section 164.528, HHS is proposing a new 164.528(b) that will provide to individuals the right to receive their electronic designated records set information. This right would not extend to access to paper records.

HHS refers to "Access Logs" and "Access Reports". The Access Log is the raw data that an electronic system containing protected health information collects each time a user as defined in the Security Rule at Section 164.304 accesses information. The Access Report is the document that a system administrator generates from the Access Log in a format that is understandable to the individual.

HITECH only addresses "disclosures" and refers to an EHR. HHS is proposing to expand the right to an Access Report to uses of information- (e.g. electronic access by members of the covered entity's workforce or the business associate's workforce) and to all electronic PHI about an individual in any designated record set.

HHS is including all electronic PHI in a designated record set rather than only EHR information. All electronic systems with designated record set information should be creating Access Logs with sufficient information to create an Access Report.

HHS does not propose to extend the Access Report requirement to paper records because HHS believes this would result in an unreasonable burden. HHS des not believe that this would be an unreasonable burden for electronic systems with designated record set information, because, according to HHS, such systems should be capable of creating Access Logs with sufficient information to create Access Reports.

The proposal of HHS to extend the right to an Access Report would cover all covered entities and business associates that maintain electronic designated record set information, including covered entities and business associates that do not have systems

that could be categorized as EHRs. HHS believes this is reasonable because HHS states that under the Security Rule covered entities and business associates are required to have Access Logs, and should be able to use Access Logs to generate Access Reports.

HHS also proposes to require covered entities to furnish reports for business associates that maintain designated record set information. In response to a request for an Access Report, a covered entity will be required to contact the business associates that create, receive, maintain, or transmit electronic designated record set information and obtain from such business associates the Access Reports with respect to the individual's information.

As in the case for Accounting for Disclosures, a covered entity only needs to obtain information from business associates that handle designated record set information. In the case of Access Reports- only electronic designated record set information.

Covered entities will need to track which business associates have designated record set information.

HHS states that it does not believe that the proposal places an unreasonable burden on business associates. Under the Security Rule, covered entities are required to include in their business associate agreements the requirement that the business associate maintain reasonable and appropriate administrative, physical and technical safeguards for electronic PHI. According to HHS, this should include the ability to determine who has accessed the electronic PHI.

Accordingly, HHS states that business associates should have the ability to create an Access Report that indicates who has accessed an individual's electronic designated record set information.

HHS is proposing that a covered entity's Access Report must include uses and disclosures by business associates of electronic designated record set information maintained by the business associate.

2. **Content of the Access Report**

CMS proposes that the Access Report must set forth:

(a) date of access;
(b) time of access;
(c) name of the natural person, if available, otherwise, the name of the entity accessing the electronic designated record set information;
(d) a description of what information was accessed, if available;
(e) a description of the action of the user, if available (such as "create", "modify", "access", or "delete").

HHS states that it believes that Access Logs include this information, so it should readily be available for inclusion in Access Reports without substantial burden to covered entities and business associates.

Comments should be forwarded to HHS regarding HHS' belief that this task is readily achievable without unreasonable burden.

General description of the action taken- HHS states that this provision is not intended to require covered entities and business associates to include in the Access Report a description of what use or disclosure was ultimately made with the information accessed or to whom the user provided the information. For example, if the purpose of the access was to provide a copy of the record to law enforcement, the Access Report should not indicate that user provided a copy of the record to law enforcement.

HHS is not proposing to require that the Access Report include a description of the purpose of the disclosure.

HHS states that it believes that there will continue to b relatively few requests for Accounting of Disclosures, but that the availability of Access Reports may lead to a greater number of requests for accounting.

HHS is not proposing that the Access Report include the ultimate recipient of the electronic PHI, unless the recipient is the natural person or entity with direct access to the electronic PHI.

HHS is proposing that covered entities must provide individuals with the option to limit the Access Report to specific date, time period, or person.

3. **Provision of the Access Report**

A covered entity would have 30 days to provide the Access Report, including the logs of the business associate that create, receive, maintain or transmit electronic designated record set information.

The covered entity must provide the individual with the Access Report in a "machine readable" or other electronic form or format requested by the individual, if it is readily producible in such form or format; or if not, in a readable electronic form or format as agreed to by the covered entity and individual. The term "machine readable" means the data is digital information stored in a standard format enabling the information to be processed and analyzed by computer.

Covered entirely may not charge for providing the first Access Report in any 12-month period, but may charge a reasonable cost-based amount for each additional Access Report in any 12-month period. The covered entity must notify the individual at the time of the first access that subsequent requests in the 12-month period may be subject to a fee.

4. **Documentation**

A covered entity of business associated must retain the documentation needed to produce an Access Report (e.g., the necessary Access Log) for 3 years.

C. **Notice of Privacy Practices 164.520**

Sections 164.520(b)(3) requires a covered entity to revise and distribute the Notice of Privacy Practice where there is a material change. The Notice of Privacy Practice must be distributed within 60 days after the material revision.

The Revised Accounting of Disclosures and Access Report requirement compliance dates are January 1, 2013 or January 1, 2014.

D. **Effective and Compliance Dates**

Covered entities will have 240 days to comply after publication of the Final Rule.

Covered entities and business associates must produce Access Report upon request beginning January 1, 2013, for any electronic designated record set system that was acquired after January 1, 2009.

A covered entity that acquired EHR after January 1, 2009, must account for disclosures for treatment payment and healthcare operations by January 1, 2013.

A covered entity that acquired EHR on or before January 1, 2009, must account for disclosures of treatment, payment and healthcare operations beginning January 1, 2014, and must produce an Access Report upon request beginning January 1, 2014.

Covered entities and business associates should already be logging access to electronic PHI and should have the ability to generate Access Reports.

Questions may be forwarded to Donald Moy,
Kern Augustine Conroy & Schoppmann, P.C.
dmoy@drlaw.com
1-800-445-0954