GROOM LAW GROUP
CHARTERED

BENEFITS BRIEF

July 13, 2011 www.groom.com

Author: Christy A. Tinnes

If you have questions, please contact your regular Groom attorney or any of the Health and Welfare attorneys listed below:

Jon W. Breyfogle
jbreyfogle@groom.com
(202) 861-6641

Elizabeth T. Dold
edold@groom.com
(202) 861-5406

Thomas F. Fitzgerald
tfitzgerald@groom.com
(202) 861-6617

Anubhav Gogna
agogna@groom.com
(202) 861-2602

Cheryl Risley Hughes
chughes@groom.com
(202) 861-0167

Christine L. Keller
ckeller@groom.com
(202) 861-9371

Tamara S. Killion
tkillion@groom.com
(202) 861-6328

Mark C. Nielsen
mnielsen@groom.com
(202) 861-5429

William F. Sweetnam, Jr.
bsweetnam@groom.com
(202) 861-5427

Christy A. Tinnes
ctinnes@groom.com
(202) 861-6603

Brigen L. Winters
bwinters@groom.com
(202) 861-6618

New Proposed HIPAA Accounting Regulation Adds Up To Big Changes for Health Plans

Comments Due 8/1/11

The Department of Health and Human Services ("HHS") recently issued a proposed rule that would change the current accounting rule under the HIPAA privacy regulations. 76 Fed. Reg. 31426 (May 31, 2011). The new rule also would require covered entities to keep a log of anyone who accesses electronic protected health information and provide an access report to individuals upon request (this requirement would apply to information held by the plan or any of its business associates). As described below, if the proposal is finalized, it would significantly impact health plans and business associates and the systems they use to maintain health information.

I. Background: The HIPAA Accounting Rule & HITECH Act

A. The Accounting Requirement under the HIPAA Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act ("HIPAA Privacy Rules") apply to covered entities – health plans, health care providers, and certain clearinghouses - and govern the use or disclosure of protected health information ("PHI"), which is defined as individually identifiable health information. Generally, the HIPAA Privacy Rules require a covered entity to obtain an individual's authorization in order to use or disclose PHI, except for the purposes of treatment, payment, or health care operations ("TPO") of the covered entity or if under a listed exception. The HIPAA Privacy Rules have explicit definitions for treatment, payment, and health care operations, which generally are the routine, day-to-day uses and disclosures a covered entity makes in treating patients and providing health coverage (for example, where a health plan performs underwriting activities, determines eligibility and claims payments, and coordinates benefits).

The HIPAA Privacy Rules include a requirement that a covered entity must track and keep an "accounting" of any use or disclosure outside of TPO, unless the disclosure is to the individual whose information is being disclosed or is a disclosure the individual has authorized. Individuals may request this accounting of disclosures for the prior six years, and the covered entity must provide the list within 60 days (subject to a 60-day extension).

Comment: Since most of a health plan's uses and disclosures likely fall under treatment, payment, or health care operations, the accounting list would include disclosures that fall under an exception to HIPAA, such as disclosures pursuant to a subpoena or to law enforcement. In our experience, participants rarely request accountings from health plans because health plans simply do not make very many disclosures outside of the routine treatment, payment, or health care operations disclosures.

B. HITECH Act's New Accounting Rule for Electronic Health Records (EHRs)

The HITECH Act, enacted in 2009, added a new accounting requirement that applies to an "electronic health record" (or "EHR"), which is defined as an electronic record or health-related information on an individual that is created, gathered, managed, or consulted by authorized health care clinicians and staff.

The HITECH Act says that a covered entity must keep an accounting of EHR disclosures, even for TPO purposes, but limited to 3 years (rather than the 6-year requirement for traditional accounting). The HITECH Act provides that a covered entity either may compile EHR disclosures by the covered entity and its business associates into a single accounting or provide an accounting of its own EHR disclosures and give individuals a list of business associates so participants can request an EHR accounting from a particular business associate.

Comment: There has been much debate about exactly what type of record would be considered an EHR and whether this rule even would apply to health plans. The definition of EHR requires that the record be created, gathered, managed, or consulted by a health care clinician. While health plans may receive records from clinicians (for example, to substantiate claims), it is not clear that these records would be considered "EHRs."

II. New Proposed Regulation Changes Accounting Rule & Adds New EHR Access Report, Even for Health Plans

On May 31, 2011, HHS issued a proposed rule that changes the current HIPAA accounting rule and adds a new EHR access report requirement that applies to all covered entities, including health plans.

A. Revised Accounting Rule

Under the proposed rule, the current HIPAA accounting rule would be changed in the following ways:

- <u>Accounting for Disclosures by Business Associates</u> – The proposed rule specifies that the accounting rule applies to disclosures made by both the covered entity and business associate. Currently, the accounting rule expressly applies to covered entities, with business associates required to comply under the business associate agreement. While the practical effect may be the same, the Preamble says the proposed rule "makes clear" that the covered entity now is responsible for coordinating with and compiling all accounting reports from business associates.

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2011 Groom Law Group, Chartered • 1701 Pennsylvania Ave NW • Washington, DC 20006. All rights reserved.

GROOM LAW GROUP CHARTERED

> *Comment: Currently, many health plans consciously seek to limit the PHI they hold and direct individuals to the applicable business associate for a request for accounting. If the covered entity is responsible for compiling this information from all of its business associates, this could be a big change from current practice. This change may be particularly difficult given the shorter deadlines for compliance under the proposed rules (see below).*

- <u>Look-Back Period Changes from 6 to 3 Years</u> – Currently, a covered entity must track applicable disclosures for the prior 6 years. Under the proposed rule, the covered entity only must track disclosures for 3 years.

- <u>Disclosures to be Tracked</u> – Currently, a covered entity must track any disclosures, except those to the individual, that the individual authorizes, or that are for TPO purposes. Generally, this means that a covered entity must track disclosures falling under an exception (e.g., law enforcement or judicial process) or disclosures not permitted under HIPAA (e.g., inadvertent non-permitted disclosures). The proposed rule further limits this list to disclosures:

  - Not permitted by the HIPAA Privacy Rule where a breach notification is not provided;
  - For public health activities (except to report child abuse or neglect);
  - For judicial and administrative proceedings or law enforcement;
  - To avert a serious threat to health or safety;
  - For military and veterans activities, the Department of State's suitability determinations, and government programs providing public benefits; and
  - For workers' compensation.

The covered entity is not required to account for disclosures under TPO or required by law (but may need to record these disclosures anyway under the new access report requirement below). The covered entity also is not required to account for disclosures outside of a designated record set (defined as records used or maintained by the covered entity to make decisions about individuals).

> *Comment: Generally, it is helpful to covered entities to further limit the disclosures that must be tracked for accounting purposes. However, some covered entities may not currently track non-permitted disclosures, except where a breach notification is required. Under the HIPAA security breach regulations, covered entities must keep a breach log (and notify the individual) where there is a non-permitted disclosure that meets certain harm thresholds. Where a covered entity determines that the disclosure does not rise to the level of a "breach," the new proposed rule would require that the covered entity list this disclosure in the accounting, essentially requiring a second breach log.*

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2011 Groom Law Group, Chartered • 1701 Pennsylvania Ave NW • Washington, DC 20006. All rights reserved.

- Content of Accounting – By and large, the content of the accounting report is the same (with slight revisions) and must include the date of the disclosure (the proposed rules allow an approximate date or range), the name of the recipient, the type of PHI disclosed, and the purpose. The proposed regulation requires that the covered entity give the individual the option to limit the accounting to a specific time period, type of disclosure, or recipient.

- Deadline to Provide Accounting – The proposed rule shortens this time period from 60 days (under the current rule) to 30 days, with a 30-day extension. The proposed rule also requires the accounting to be provided in a form and format requested by the individual, "if readily producible." The Preamble says this means that the individual may request the accounting in PDF form or a particular software.

- Free of Charge – As under the current rule, the first accounting in a 12-month period must be free of charge. After that, the covered entity may charge a reasonable, cost-based fee for each subsequent accounting (the Preamble notes that this may be a reason the individual may limit the request to a shorter time period or type or may request a particular format, in order to limit the cost.)

- Effective Date – The proposed accounting rule provisions will be effective 240 days after a final rule is published in the Federal Register.

B. Access Report for All Electronic PHI (Not Just EHRs)

HHS proposes a new requirement that all covered entities – even health plans - must provide an access report upon request for any use or disclosure of electronic PHI in a designated record set. This new requirement would go significantly beyond the mandate in the HITECH Act that this type of provision only apply to EHRs. In the Preamble to the proposed rule, HHS recognizes it is going "beyond the statutory provision," but says it feels this expansion of authority is "reasonable."

The proposed rule would require covered entities to provide an access report that describes any use or disclosure of electronic PHI as follows:

- All Electronic PHI (Not Just EHRs) - The access report must include all uses and disclosures of electronic PHI for the prior 3 years, even for TPO functions and even information accessed internally.

- Designated Record Set - The requirement applies to information in a designated record set, defined as records used or maintained by the covered entity to make decisions about individuals, including the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan. The Preamble says that peer review files, for example, would not be used to make a decision about an individual, so are not part of a designated record set. (Most information held by a health plan likely will be part of a designated record set.)

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2011 Groom Law Group, Chartered • 1701 Pennsylvania Ave NW • Washington, DC 20006. All rights reserved.

Comment: Several times in the Preamble to the rules, HHS notes that covered entities already must maintain access logs under the HIPAA security rule and seems to think that it will be simple to convert these access logs into an access report that is understandable to individuals. Typically, access logs are reports able to be generated by the IT department and often in some type of code format. These codes usually are not easily translated or universally able to be sorted (as seems to be suggested by HHS).

- Access by Covered Entity & Business Associate – The covered entity also must compile the access reports for any business associates.

Comment: HHS goes beyond the HITECH Act both in extending this rule to all electronic PHI (not just EHRs), but also in including business associates. The HITECH Act expressly allows a covered entity to direct individuals to a list of business associates, rather than compile all of this information itself. HHS justifies this expansion by saying, "[W]e are exercising our general authority under the HIPAA statute . . . ."

- Content of Access Report - The access report must list the date of access, time of access, the name of the person accessing the information (or entity if unavailable), description of information accessed, and description of the action taken (e.g., create, modify, access, delete, print).

- Multiple Systems Must Be Aggregated – Where a covered entity and business associate have more than one system that may capture this information, the proposed rule requires the covered entity to aggregate this information into a single report. HHS recognizes this may cause a "significant burden," but says it believes it is reasonable in the interest of individuals.

- Deadline to Create - The access report must be provided within 30 days (with a 30-day extension) in a form and format requested by the individual, "if readily producible." As with the proposed accounting rule, the Preamble says this means that the individual may request the accounting in PDF form or a particular software.

Comment: This deadline includes not only the covered entity compiling its own access report, but also coordinating and obtaining logs from all of its business associates. Some health plans have dozens of business associates who administer claims for participants in various geographic regions, along with EAPs, wellness vendors, pharmacy benefit managers, consultants, and even outside counsel. It will be very difficult to obtain this information and compile in a single, non-aggregate, readable report in a format requested by the individual – all within 30 days.

- Free of Charge - The first access report in a 12-month period must be free of charge. After that, the covered entity may charge a reasonable, cost-based fee for each subsequent access report.

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2011 Groom Law Group, Chartered • 1701 Pennsylvania Ave NW • Washington, DC 20006. All rights reserved.

- Effective Date – For electronic designated record set systems acquired after 1/1/09, the new requirement will apply as of 1/1/13. For electronic designated record set systems acquired on or before 1/1/09, the new requirement will apply as of 1/1/14. Covered entities also will be required to reflect this new right in their HIPAA privacy notices.

III. Comments

Comments on the proposed rule are due 8/1/11. HHS poses several specific questions throughout the Preamble on both the accounting rule revisions and the new access report requirement. Health plans and business associates should take note of these proposed requirements, consider whether to comment, and watch for future regulation.

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2011 Groom Law Group, Chartered • 1701 Pennsylvania Ave NW • Washington, DC 20006. All rights reserved.