HOBBS
STRAUS
DEAN &
WALKER

806 SW Broadway, Suite 900
Portland, OR 97205

T 503.242.1745
F 503.242.1072

HOBBSSTRAUS.COM

MEMORANDUM

February 6, 2013

TO: Health Clients

FROM: Geoff Strommer & Starla Roels
HOBBS, STRAUS, DEAN & WALKER, LLP

RE: ***Big Changes to HIPAA Requirements – The Megarule***

The Department of Health and Human Services' (DHHS) Office for Civil Rights (OCR) issued major changes to the Health Insurance Portability and Accountability Act (HIPAA) regulations on January 25, 2013: *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules,* 78 FED. REG. 5566 (Jan. 25, 2013). The pre-publication version released a few days earlier by the OCR topped 550 pages of what has come to be called the "omnibus" rules, or more colorfully, the "HIPAA Megarule."

The HIPAA Megarule implements changes to several provisions within the HIPAA Security, Privacy and Enforcement rules, modifies the interim final rules that were previously issued to address breach notification requirements, changes the interim final enforcement rules, and revises the HIPAA regulations to implement the Genetic Information Nondiscrimination Act (GINA). Because of the large scope of the Megarule, we focus in this memorandum on the primary changes we think will be most important to our tribal health clients. ***At a minimum, the Megarule will require revisions to your HIPAA policies and procedures, Notice of Privacy Practices, and likely also your Business Associate Agreements.*** For this memorandum, we focus on the following topics:

- Revisions that will need to be made to the Notice of Privacy Practices;
- The new approach to an individual's access to health information, including when the individual directs the Covered Entity to send Protected Health Information (PHI) to a third-party;
- The revised breach notification rules, including a new presumption of breach and a change to the risk assessment requirements;
- Significant changes for Business Associates of a Covered Entity;
- The simpler requirements for disclosure of immunization records;
- Changes in the way in which records of a decedent are treated;

- New limitations on a Covered Entity's treatment of an individual's request for restrictions on use or disclosure of PHI;
- The parameters governing sale of PHI;
- Limitations on use or disclosure of PHI for fundraising or marketing activities;
- Increased flexibility of using PHI for research; and
- Changes made to the enforcement and penalties for failure to comply with the HIPAA rules, as amended.

The Megarule becomes effective on March 26, 2013. Covered entities and Business Associates have until September 23, 2014 to comply with most of the regulatory provisions. Other compliance dates are specifically mentioned below.

Revisions Required To Notice of Privacy Practices

The Megarule requires a Covered Entity to include additional statements in the entity's Notice of Privacy Practices. The Notice must inform individuals of the Covered Entity's duty to notify affected individuals of a breach of unsecured PHI (see more on the breach notification rules below). The statement on an individual's right to request restrictions on certain uses and disclosures of PHI should be updated to explain that the Covered Entity is not required to agree to a requested revision *except* that the Covered Entity may not refuse a request to withhold information from a health plan when the individual pays in full for the service.

The Notice must be updated to include a description of the types of uses and disclosures of PHI that require a patient's authorization (per 45 C.F.R. §§ 164.508(a)(2)-(a)(4)). DHHS explains in the publication of the rule that this includes most uses and disclosures of psychotherapy notes (where appropriate), for marketing, and for the sale of PHI – all of which require authorization. If it does not already do so, the Notice should include a statement that other uses and disclosures not specifically described in the Notice will be made only with the individual's authorization.

Separate statements must also be included, as applicable. For example, if a Covered Entity anticipates engaging in fundraising activities, the Notice must explain that the Covered Entity may contact the individual for fundraising and the individual has a right to opt out of receiving such fundraising communications. For health plans that use PHI for underwriting purposes, the Notice must state that the plan is prohibited from using and disclosing genetic information for underwriting purposes.

Under the Megarule, the Notice no longer has to contain a statement about appointment reminders or information about treatment alternatives. Those statements may be deleted from your Notices. As you work on making these revisions, it is a good time to ensure that your Notices accurately describe your actual privacy practices.

The Megarule thus requires that certain changes be made to your Notice of Privacy Practices and that such revised Notices be redistributed. For health care providers, recall that they must "promptly" revise and distribute the revised Notice whenever there is a material change. For health plans, the Megarule includes some flexibility for distribution of revised Notices. If the health plan prominently posts its Notice of Privacy Practices on its website, then it must post the revised Notice by the date of the material change, and then include the revised Notice (or information about the revised Notice) in the plan's next annual mailing to its participants. However, if the health plan does not post its Notice on a website, then it must provide the revised Notice (or information about the revised Notice) to covered individuals within 60 days of the material change.

Individual's Access to PHI

The HIPAA Megarule made two significant changes to an individual's rights to access PHI. First, if an individual requests a copy of his or her PHI that is maintained electronically in a designated record set, the Covered Entity must provide the individual with electronic access in the form and format as requested by the individual. However, if the PHI is not readily producible in that form or format, but is maintained electronically, the Covered Entity must produce a readable electronic copy as mutually agreed by the Covered Entity and the individual, and can only charge for labor and cost of the electronic media. If the PHI is not readily producible in the requested form and format and is maintained on paper, then the Covered Entity must produce a readable hard copy.

Second, if an individual requests that the Covered Entity send PHI to a designated third party, the Covered Entity must send the information to that party. ***The individual no longer must fill out and sign a HIPAA-compliant authorization form***, however, they still have to sign a written request that clearly identifies the third-party and where to send the PHI.

Breach Notification Rules

The HITECH Act requires notification to individuals and the Secretary of DHHS about breaches of unsecured PHI. Under the interim final rules that implemented that requirement, DHHS imposed a risk assessment process for determining "risk of harm" to the individual. The risk assessment was part of the decision-making process for determining whether a breach occurred and notice must be provided.

Under the HIPAA Megarule, the definition of "breach" continues to be viewed as an unauthorized acquisition, access, use, or disclosure of unsecured PHI in a manner that is not permitted by the HIPAA Privacy Rule and that compromises the security or privacy of the PHI. However, the Megarule now establishes a presumption that any such unauthorized use or disclosure of PHI is a breach. That presumption stands unless the

Covered Entity can demonstrate that there is a "low probability that the [PHI] has been compromised based on a risk assessment."

In order to demonstrate such low probability, the Covered Entity or Business Associate (Business Associates must have their own breach notification policies) would need to undertake a documented risk assessment that looks at four mandatory factors: the nature and extent of the PHI involved, the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated. A Covered Entity can look at additional factors too, but must evaluate the overall probability and make reasonable conclusions. DHHS unfortunately did not define "compromise" and has promised more guidance on that term in the future. The burden of proof for not providing notification – based on the outcome of the risk analysis – remains on the Covered Entity or Business Associate.

The primary changes to the breach notification requirements were thus to presume breach and replace the analysis of the "risk of harm" to an individual with the standard of low probability of compromise. Additionally, the Megarule gives Covered Entities and Business Associates the discretion to provide the breach notification to the individual, based on the presumption there was a breach, and thereby skip having to perform the risk assessment. In other words, the risk assessment does not have to be done if you decide to provide the notification.

Requirements for what must be addressed in the notification letter to the individual were not changed by the Megarule. The timing for when notice must be provided was revised for notification to DHHS for breaches affecting less than 500 people – it now must be provided within 60 days of the end of the calendar year in which the breach was discovered (as opposed to when the breach occurred). ***Covered entities and Business Associates will need to review and likely revise their breach notification policies to reflect the new rules.***

Business Associates

The HIPAA Megarule broadens the definition of a "Business Associate" of Covered Entities. Business Associates and their subcontractors are now directly liable to DHHS for compliance with HIPAA safeguards, such as the security rules (administrative, physical, and technical safeguards), and breach notification rules. Business Associates are no longer only contractually liable to Covered Entities, and must fully implement their own policies and procedures that comply with the new rules. A Covered Entity is also now made specifically liable for violations of its Business Associates who are a Covered Entity's "agents" under the federal law of agency.

Business associate agreements (BAAs) must be updated to reflect the requirements of the HIPAA Megarule. BAAs must contain satisfactory assurances and

meet the minimum content requirements found in the privacy and security rules, as amended. The BAAs must also establish the uses and disclosures of PHI that will be covered within its scope (e.g., as required and as permitted by HIPAA's Privacy rule). BAAs must be consistent with how the Covered Entity itself may use or disclose PHI in accordance with the Privacy Rule, subject to a few exceptions. If a Business Associate will carry out the obligation of a Covered Entity under the Privacy Rule, then the Business Associate must itself comply with the Privacy Rule requirements that apply to the Covered Entity in performing that obligation. The BAA must also specify that a Business Associate will utilize appropriate safeguards for PHI and comply with the HIPAA Security Rule for electronic PHI. Business Associates now have an obligation to comply with HIPAA's breach notification requirements and to accordingly report breaches.

All BAAs must be revised to be compliant with these new requirements by the September 2013 compliance deadline, except that there are grandfathering provisions for certain existing BAAs: BAAs in existence as of January 25, 2013 that (a) meet all of the HIPAA Security and Privacy Rule requirements, and (b) are not renewed or modified between March 26, 2013 and September 23, 2013, may have an additional year to comply (to September 22, 2014).

The Megarule expands the definition of "Business Associate" as anyone who creates, receives, maintains, or transmits PHI for a function regulated by the rules. Notably, the rule includes in the definition entities that maintain, but do not access, PHI. Business Associates now include claims processors, administrators, data analysts, individuals or entities performing quality assurance activities, and persons conducting patient safety activities (individuals that perform these activities as *members of the workforce* of a Covered Entity are not Business Associates). 45 C.F.R. § 160.103(1)(i). Additionally, the new definition brings within its scope any person or entity that provides "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services," for a Covered Entity if the service provided involves any disclosure of PHI. 45 C.F.R. § 160.103(1)(ii).

The Megarule also expressly includes health information organizations, E-prescribing Gateways, and any other person that "provides data transmission services with respect to [PHI] to a covered entity and that requires access on a routine basis to such [PHI];" a person that "offers a personal health record to one or more individuals on behalf of a covered entity;" and a "subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." 45 C.F.R. § 160.103(3)(i)-(iii).

As noted above, the new rule includes subcontractors of Business Associates within its scope. The rule defines a subcontractor as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." 45 C.F.R. § 160.103. Business Associates

must enter into Business Associate Agreements with their subcontractors, and those subcontractors must also comply with the new rules. Thus, the new rule is broad enough that it captures within its purview all Covered Entities, Business Associates, and all "downstream" persons or entities within its purview.

Immunization Records

One area where the Megarule has made life easier for providers and patients pertains to student immunization records. A Covered Entity may now release student immunization records without needing patient authorization if (a) state law requires the school to have the immunization record, and (b) the Covered Entity can document that it has oral or written agreement from the individual or the individual's parent/legal guardian for the disclosure.

Decedents

Another area of increased flexibility under the Megarule pertains to decedents. A person's health information is no longer considered PHI (and thus is no longer subject to the HIPAA privacy rule) 50 years after death. Additionally, a Covered Entity can now disclose PHI to persons involved in a decedent's care or payment, so long as doing so is not contrary to the individual's prior expressed preference.

Requests for Restriction

Under the old HIPAA rules, Covered Entities can refuse to agree to an individual's request for restriction on the use or disclosure of PHI that is otherwise allowed under HIPAA. The Megarule created a new limitation requiring Covered Entities to agree to restrict disclosure to a health plan for payment or health care operations purposes (unless disclosure is required by law) when the individual or someone on the individual's behalf pays for the item or service in full – out of pocket.

Sale of Protected Health Information

Under the HITECH Act, Congress prohibited the sale of PHI – a Covered Entity cannot receive any remuneration in exchange for PHI – with certain limited exceptions. The Megarule explains the exceptions as including treatment or payment purposes; due to the sale, transfer, merger or consolidation of a Covered Entity and related due diligence; or when required by law. The Megarule allows Business Associates to be paid by the Covered Entity for activities that the Business Associate performs on behalf of the Covered Entity. Sale of PHI is also allowed in certain additional situations with specific limitations, including for research, providing health information to the individual who is the subject of the information, and for any other allowable purpose under HIPAA if the remuneration is limited to a reasonable, cost-based charge for the preparation and transmission of the PHI.

Limits on Fundraising and Marketing

Under the HIPAA Megarule, communications about fundraising must include very clear and conspicuous notice of the individuals' ability to opt out of receiving further fundraising communications. The opt-out process must not be burdensome, and a Covered Entity may provide a method for individuals to opt back in. The Covered Entity may not condition treatment or payment on the individual's agreement to receive such communications. Once an individual opts out, the Covered Entity may not make any further fundraising communications, unless and until the individual opts back in. The good news is that the Megarule allows a broader scope of PHI for fundraising purposes. For example, the Megarule now allows Covered Entities to use the treating physician's name, department of service, outcome information and health insurance status.

The general rule on marketing is that a communication about a product or service that encourages its purchase or use is marketing and requires the individual's authorization. Under the old HIPAA regulations, there was an exception to this general rule for treatment and health care operations. The HIPAA Megarule modifies that exception where the Covered Entity receives financial remuneration from the third party whose product or service is described – that is considered marketing. The Megarule added a new exception, such that marketing does not include refill reminders about a drug that is being prescribed, so long as the remuneration is reasonably related to the cost of the communication.

Research

The Megarule includes increased flexibility for researchers. As one example, a single authorization can be used to cover uses and disclosures for two different research studies. Covered entities can now combine "conditioned" (e.g., for clinical trial) and "unconditioned" (e.g., tissue specimen repository) authorizations, subject to certain requirements and limitations.

Genetic Information

The Megarule adopts changes made to HIPAA by GINA. The Megarule clarifies that genetic information is health information and specifies that a health plan other than a long-term care plan may not use or disclose genetic information for underwriting purposes.

Enforcement and Penalties

The HIPAA Megarule now requires the Office of Civil Rights (OCR) to investigate any HIPAA complaint received when a preliminary review of the facts shows there is a possible violation due to "willful neglect." The term "willful neglect" is

defined to mean conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA. While the OCR has discretion not to investigate if it preliminarily thinks there is no willful neglect, the OCR has indicated that it "conducts a preliminary review of every complaint received and proceeds with an investigation in every eligible case where the facts indicate a possible violation of the HIPAA Rules." Under the Megarule, OCR will also conduct compliance reviews to determine whether a Covered Entity or Business Associate is complying with the applicable HIPAA rules.

The enforcement regulations continue to provide that OCR "may" try to resolve complaints or problems identified during compliance reviews, but the Megarule gives the OCR greater discretion to proceed directly to imposing penalties. Additionally, Covered Entities may now be held vicariously liable for violations of certain of their Business Associates under the federal law of "agency," as noted above.

Still to Come

The HIPAA Megarule does not address other outstanding issues that will be separately addressed by DHHS in future rulemaking. These include revisions to requirements on accounting for disclosures, guidance on the minimum necessary standard, and the distribution of penalties or settlements to harmed individuals. We will continue to monitor HIPAA-related issues and report to you in the future.

A copy of the HIPAA Megarule can be found at www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

If you would like more detailed information about any of the topics discussed in this memorandum or any other changes made to HIPAA through the Megarule, or if we can provide any assistance with reviewing or assisting with redrafting any of your policies, Notices or Business Associate agreements, please contact Geoff Strommer or Starla Roels at 503-242-1745, gstrommer@hobbsstraus.com; sroels@hobbsstraus.com.