Health Law Advisory

February 28, 2013 • Julie A. Knutson, Editor

BAIRD HOLM LLP
ATTORNEYS AT LAW

The Next Decade of HIPAA: Omnibus Final Rule Brings Challenges and Increased Enforcement

As we near the ten year anniversary of covered entities complying with the original HIPAA Privacy Rule (April 14, 2003), the Office for Civil Rights (OCR) has issued a wake-up call with the publication of a consolidated final rule implementing new and enhanced standards for *Privacy, Security, Enforcement and Breach Notification* as required by the HITECH Act ("Final Rule").[1] The Final Rule, often referred to as the "omnibus rule" in reference to the publication of four final rules simultaneously, makes sweeping changes to HIPAA as we know it, and increases penalties for non-compliance. The Final Rule is comprised of the following four final rules:

- Final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules mandated by the HITECH Act, and certain other modifications which were issued as a proposed rule on July 14, 2010.

- Final rule adopting changes to the Enforcement Rule to incorporate the increased and tiered civil monetary penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

- Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

- Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act of 2008 ("GINA") to prohibit health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

Except as noted below with respect to compliant business associate agreements in place prior to January 25, 2013, covered entities are required to comply with the Final Rule by September 23, 2013.

Increased Penalties and Enhanced Enforcement

Some of the most significant provisions of the Final Rule are in the area of penalties and enforcement. The HITECH Act established four tiers of violations that reflect increasing levels of culpability with corresponding penalty amounts that increased with each tier, and made those provisions effective immediately as to violations occurring after the enactment date of February 18,

1 "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 (January 25, 2013).

2009. The Final Rule adopts the changes originally made in the proposed rule and interim final rule, with some modifications, and signals OCR's intent for increased enforcement in the comments to the Final Rule.

OCR indicated that where multiple individuals were involved in a breach, the number of violations of the privacy rule standard regarding permissible uses and disclosures would be counted by the number of individuals involved.

Willful Neglect. The HITECH Act added the requirement for the Secretary to investigate any allegation which appears, based on a preliminary investigation of the facts, to be a violation of HIPAA due to "willful neglect." The HITECH Act also mandated that the Secretary impose a penalty for violations that are found to be due to "willful neglect." The Final Rule implements these requirements and confirms that the Secretary will investigate any complaint when a preliminary review of the facts indicates a possible violation due to willful neglect, and may investigate any other complaint. The penalty tiers for violations are unchanged from the HITECH Act, ranging from $10,000 - $50,000 per violation, up to $1.5 million for identical violations in a year. Whether or not OCR finds the violation to be due to willful neglect carries significant consequences. First, if the violation is not due to willful neglect and is corrected within 30 days of the entity's knowledge of a violation, OCR is prohibited from imposing a penalty. This is a powerful provision and must be acted on quickly by covered entities following any discovery of a violation. Secondly, if the violation is due to willful neglect and is corrected within 30 days, the penalty tier is lower than for those violations due to willful neglect that are not corrected. Importantly, OCR does not have the authority to waive the imposition of penalties if there is a finding of willful neglect.

Counting Violations. In response to questions from commenters, OCR clarified how the number of occurrences would be counted for purposes of imposing civil monetary penalties. Generally speaking, OCR indicated that where multiple individuals were involved in a breach, the number of violations of the privacy rule standard regarding permissible uses and disclosures would be counted by the number of individuals involved. Thus, a breach involving 100 patients would be considered 100 violations. OCR also indicated that the number of violations for an on-going deficiency, such as failure to post an updated Notice of Privacy Practices on a covered entity's website, would be counted on a per-day basis. OCR also confirmed that a particular incident in which patient information was breached would likely involve violation of numerous standards, for each of which OCR can calculate a separate civil monetary penalty.

Covered Entities Liable for the Actions of Its Business Associates. One of the most significant changes in the Final Rule is the removal of an exception that had previously been available to covered entities. Prior to this Final Rule, covered entities could not be held liable for the acts of its agent in cases where the agent is a business associate, the requirements of having a compliant business associate agreement in place were met, and the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act to end the violation or terminate the business associate agreement. With the removal of this exception, the Final Rule provides that a covered entity is liable for the acts of its agents acting within the scope of agency (under the Federal common law of agency), regardless of whether or not the covered entity had a compliant business associate agreement in place with the entity.

The preamble commentary to the Final Rule notes that the determination of whether a business associate is acting as an agent will be case-specific, taking into account the terms of the business associate agreement as well as the "totality of the circumstances involved in the ongoing relationship between the parties." The primary factor that OCR will look to is the right or authority of a covered entity to control the business associate's conduct in performing its services. The preamble provides:

"The authority of a covered entity to give interim instructions or directions is the type of control that distinguishes covered entities

in agency relationships from those in non-agency relationships…. Specifically, if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent."

Each underlying service agreement with the business associate must be evaluated to determine whether the business associate is acting as an agent under this strict interpretation by OCR. In addition, the business associate agreement could also create an agency relationship where one otherwise did not exist. The preamble to the Final Rule states:

"For example, if the terms of a business associate agreement between a covered entity and its business associate stated that "a business associate must make available protected health information in accordance with 164.524 based on the instructions to be provided by or under the direction of a covered entity, then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship."

This is a common provision in many business associate agreements that covered entities must now be wary of, or face potential liability attributed to the covered entity for the improper acts of the business associate. The Final Rule preamble also confirms that, even if the business associate violates the business associate agreement, it will generally still be acting within the scope of agency as long as it was undertaking to perform the contracted services, even if it did so negligently. If the business associate's improper conduct was for its own personal benefit or not for any purpose of the covered entity, the conduct may be determined to be outside the scope of the agency relationship.

The covered entity or business associate is now required to apply a four-part risk assessment to determine whether or not the PHI has been compromised in a manner constituting a breach.

New Standard for Triggering Breach Notification

The data breach notification duty is triggered by a breach of unsecured PHI. Breach continues to be defined to mean:

"The acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."

In the Final Rule, OCR has removed the prior test for determining whether an incident "compromises" the security or privacy of PHI. The prior test turned on whether or not the incident "poses a significant risk of financial, reputational, or other harm to the individual." OCR viewed this test as too subjective – as placing the covered entity in the role of determining what will or will not harm the individual.

The Final Rule creates a *presumption* that an acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is a breach, unless the covered entity or business associate demonstrates that there is a *low probability* that the PHI has been compromised. The covered entity or business associate is now required to apply a four-part risk assessment to determine whether or not the PHI has been compromised in a manner constituting a breach. The four components of the risk assessment, each of which must be considered, given weight and documented, are:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the PHI was disclosed;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Deciding how to apply the new standard to the risk assessment process will likely occupy many months of debate and dialogue within covered entities. OCR promises further guidance, but with no timetable.

The four-part test clearly retains a strong element of subjective determination of harm to the individual (or perhaps that remains the main focus, but only following

a more carefully crafted series of risk analysis steps). Covered entities will start with the presumption that PHI has been compromised, will consider and give weight to each of the four listed risk factors, and must be comfortable documenting that there is a "low probability that the [PHI] has been compromised" in order to avoid breach notification. This change materially heightens the risk to covered entities and business associates when they choose not to report, and puts an even greater premium on documentation of results of investigation and thought processes.

Changes Impacting Business Associates (and now their Subcontractors)

The Final Rule has a significant effect on business associates and their subcontractors. The HITECH Act made parts of the Security Rule, Privacy Rule and the Breach Notification Rule applicable directly to business associates. The Final Rule implements the HITECH Act provisions and clarifies how those provisions will be applied to business associates.

Expanded Definition of Business Associate. The Final Rule made several changes to the definition of business associate. First, the Final Rule expands the definition to include the following types of entities:

A Health Information Organization, E-prescribing Gateway, or 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

- A subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate (discussed in detail below)

OCR confirmed it would be a fact-specific analysis to determine which business associates require access on a routine basis as opposed to being mere conduits. They clarified that the conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or UPS, and their electronic equivalents, such as Internet Service Providers (ISPs) providing mere data transmission services. The conduit exception does not apply to entities that maintain or store information on behalf of covered entities, even if the entity does not view the data. To ensure no ambiguity, the Final Rule modifies the definition of business associate to include anyone who creates, receives, *maintains*, or transmits PHI on behalf of a covered entity.

Subcontractor Business Associates. The definition of business associate also expands the requirements of HIPAA to all subcontractors of business associates, thus making the chain of business associates *ad infinitum*. OCR states the purpose of this provision is to "avoid having privacy and security protections for PHI lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity." Business associates are *required* to have subcontractor business associate agreements in place with each downstream entity that creates, receives, maintains or transmits PHI at the direction of or on behalf of a business associate. Covered entities are not required to have an agreement in place with subcontractor business associates.

Business associates are required to have subcontractor business associate agreements in place with each downstream entity that creates, receives, maintains or transmits PHI at the direction of or on behalf of a business associate.

Business Associate Agreements and Direct Liability. Business associates are statutorily liable for complying with the majority of the Security Rule and the Breach Notification Rule. The preamble notes that the HITECH Act did not create direct liability for business associates with regard to compliance with *all* requirements under the Privacy Rule. The Final Rule confirms that business associates are only directly liable for uses and disclosures that are not in accord with its business associate agreement or the Privacy Rule. In addition, a business associate is directly responsible to provide its books and records to the Secretary for determining compliance with HIPAA, for providing information to the covered entity as is necessary for a covered entity to comply with the individual's right to access

PHI electronically, for meeting the minimum necessary requirements, and for entering into business associate agreements with its subcontractors. The business associate remains contractually responsible to comply with all Privacy Rule requirements found in the business associate agreement.

Business associate agreements must be amended to require that the business associate comply with the Security Rule obligations with respect to ePHI and to report breaches of unsecured PHI to the covered entity. The business associate agreements must also be amended to require business associates to enter into subcontractor business associate agreements with each of its subcontractors. Business associate arrangements should be evaluated to determine whether the business associate will carry out any of the covered entity's duties with respect to meeting the individual rights requirements of the Privacy Rule (such as distributing the Notice of Privacy Practices for the covered entity) or any of the elements of the Breach Notification Rule (such as provide the breach notification to individuals). The implications of the business associate becoming an agent of the covered entity for these purposes must be carefully considered.

If the covered entity and business associate had a compliant agreement in place prior to January 25, 2013 (and they do not amend it in the interim), the existing agreements are grandfathered for an additional year (September 23, 2014) before modification to meet the Final Rule is required.

New Rules for Fundraising

Prior to the Final Rule, covered entities were permitted to use, or disclose to an institutionally related foundation or a business associate, limited PHI including demographic information and dates of service. The Final Rule makes several changes to the fundraising rules. The categories of PHI that may be used or disclosed now include:

- Demographic information (including name, address, other contact information, age, gender, and date of birth);
- Dates of health care provided;
- Department of service information (general department of treatment – e.g., cardiology or pediatrics);
- Treating physician;
- Outcome information (including death or sub-optimal treatment); and
- Health insurance status.

Covered entities must include the intent to make fundraising communications in the notice of privacy practices. In addition, *all* fundraising communications (including phone calls) must include a clear and conspicuous opportunity for the individual to elect not to receive future fundraising communications. The opt-out method must not cause the individual an undue burden, and OCR recommends mechanisms such as a toll-free number, e-mail address, or pre-paid post card. Covered entities may not make fundraising communications to an individual who has elected not to receive communications. The Final Rule replaced the previous requirement that the covered entity make "reasonable efforts" to ensure that communications are not sent to an individual who has opted out.

Covered entities cannot condition treatment or payment on an individual's decision to opt-out of receiving fundraising communications. Finally, covered entities must provide individuals an opportunity to opt back in to the receipt of fundraising communications. The Final Rule gives covered entities flexibility in implementing many of the fundraising rules. Therefore, it is important to revise existing policies and ensure that adequate data management systems are in place to trace an individual's status concerning fundraising communications.

Stricter Marketing Standards

Prior to the Final Rule, covered entities were required to obtain an individual's authorization before using or disclosing PHI to market a third party's product or service to the individual. The Privacy Rule, however, excluded certain communications from the definition of "marketing," including communications about treatment or health care operations, even if the covered entity received remuneration from a third party to make the treatment communication. Under the Final Rule, an authorization is now required for *all* subsidized marketing communications where the covered entity (or a business associate) receives financial remuneration for the purpose of making a communication to encourage individuals to purchase or use a third party's product or

service. The authorization of the individual must be obtained before any use of the data begins for marketing purposes, and the authorization must explain the financial remuneration involved.

The authorization of the individual must be obtained before any use of the data begins for marketing purposes, and the authorization must explain the financial remuneration involved.

Financial remuneration includes direct (from the third party) and indirect (from an entity on behalf of the third party) payments to market the third party's product or service. Face-to-face communications made by the covered entity to an individual and promotional gifts of nominal value from a covered entity to an individual are still not treated as marketing. Also, the Final Rule states that the following communications are not considered marketing (and therefore no authorization is required): (1) refill reminders (including communications about generic equivalents), provided the remuneration is reasonably related to the cost of the communication; (2) communications to promote health in general; and (3) communications about government-sponsored programs.

Sale of PHI Prohibited

The Final Rule adopts HITECH's prohibition on the sale of PHI; and, absent an authorization from the individual, prohibits a covered entity (or business associate) from disclosing PHI if the covered entity (or business associate) receives remuneration in exchange for the PHI. A "sale" encompasses more than the transfer of ownership, and may include access, license, or lease agreements. A sale occurs when a covered entity (or business associate) is being compensated (through financial or non-financial/in-kind benefits) in exchange for PHI it maintains in its role as a covered entity (or business associate). OCR clarified that PHI exchanged through a health information exchange ("HIE") is not a sale, as the remuneration paid is for HIE services, not PHI. The Final Rule *allows* the exchange of remuneration and PHI for:

- Public health purposes (e.g., voluntary public health reporting);
- Research disclosures (e.g., when a covered entity receives a reasonable cost-based fee to transmit PHI to a research study sponsor);
- Treatment and payment purposes;
- The transfer, merger or consolidation of a covered entity with another covered entity (including the related due diligence);
- Disclosures required by law;
- Providing an individual with access to his or her PHI or an accounting of disclosures;
- A covered entity's payment to a business associate for activities performed on behalf of the covered entity; and
- A covered entity's receipt of reasonable cost-based fees to cover the cost to prepare and transmit PHI for any other disclosure otherwise permitted by the Privacy Rule.

Enhanced Individual Rights

The Final Rule adopts most of the expanded individual rights first introduced in the HITECH Act.

Mandatory Restrictions on Disclosures to Health Plan. Individuals have the right to request that a provider restrict the disclosure of PHI about the individual to a health plan if the disclosure is for payment or health care operations purposes (and is not otherwise required by law) and the PHI pertains solely to a health care item or service for which the individual, or someone paying on the individual's behalf, has paid the covered entity in full. Operationalizing this new provision may one of the toughest challenges of the Final Rule. The preamble notes that providers are not required to create separate medical records or otherwise segregate PHI subject to a restricted health care item or service; however, providers will need to employ some method to flag PHI in the record that is subject to a restriction. The preamble provides significant guidance to providers on the requirements as they relate to, for example, Medicare/Medicaid beneficiaries, bundled services where the individual only requests a restriction as to one element of the bundled claim, providers operating in an HMO that are restricted from billing the patient above the individual's cost-sharing amount, pre-certification issues, requests after care has been

initiated, and similar challenging situations. Providers should carefully review the preamble discussion as it develops its procedures for implementing this requirement.

Electronic Copies of PHI. If PHI is maintained in an electronic designated record set and the individual requests an electronic copy of such information, the covered entity must provide the individual with access in the electronic form and format requested by the individual, if it is readily producible in such form and format. If the format requested by the individual is not readily producible, the covered entity and individual can agree on an alternate "machine readable" electronic format (e.g., MS Word, Excel, text, HTML or text-based PDF), as long as it is available in some electronic format. The preamble comments indicate that some covered entities may be required to purchase software or hardware upgrades to satisfy this requirement for some electronic format on legacy systems. The covered entity must produce all electronic information in a designated record set. This is an expansion from the HITECH Act which only required access to information maintained in an EHR. If the designated record set includes electronic links to images or other data, the images or other data that is linked to the designated record set must also be included in the electronic copy provided to the individual. The electronic copy must contain all information maintained electronically in a designated record set at the time of the request, but does not require the covered entity to convert any portion of a designated record set that is only maintained in paper format to an electronic format for purposes of the request.

There is flexibility in how the covered entity accommodates this new provision. They could provide a disc or USB drive with a PDF file, provide access through a web-based portal, or send a copy of the medical record via e-mail. If the individual does not accept any of the electronic formats that are readily producible, the covered entity may satisfy its requirement through a hard copy of the record. Covered entities are not required to accept electronic media supplied by the patient as such devices can introduce significant security risks into the covered entity's system. However, covered entities are not permitted to require the individual to purchase electronic media (such as a USB drive) from the covered entity, if the individual would prefer to receive the information via e-mail or another available electronic format.

The preamble also notes that covered entities, in providing the individual with an electronic copy of PHI through a web-based portal, email, on portable electronic media, or other means, must ensure that reasonable safeguards are in place to protect the information. The covered entity can send the information via unsecured e-mail at the individual's request, as long as the covered entity has advised the individual of the risk that the PHI could be intercepted and viewed by a third party. Covered entities are not responsible for the information once it is delivered to the individual.

Transmission to Third Parties. A corollary provision also allows individuals to direct the covered entity to transmit an electronic copy of its record to a third party, as long as the request is in writing and clearly identifies the designated person and where to send the information.

Fees. Covered entities can include the labor costs of skilled technical staff required to create and copy the electronic file, such as compiling, extracting, scanning and burning PHI to media and distributing the media. The cost of supplies, such as a USB drive or CD can be included if the individual requests information in that format.

Timeliness for Access to PHI. The time allowed for a covered entity to respond to a request for access (both paper and electronic) has been shortened to 60 days (30 day initial response time with one 30 day extension allowed). We note that, for providers attesting, or preparing to attest to meaningful use requirements, the timeline for providing an electronic copy are much shorter.

What's Missing? Final rules for expanded accounting of disclosures of PHI for treatment, payment and health care operations required under the HITECH Act are were not part of the Final Rule and are still pending release by OCR.

Changes to the Notice of Privacy Practices

The Final Rule triggers two types of changes to the notice of privacy practices (NPP). There are changes required to address specific regulatory content added

by the Final Rule. There are also changes that are advisable, if not mandatory, to more completely describe how use and disclosure policies and individual rights policies will likely change, based on substantive amendments in the Final Rule.

Remember, the NPP has enormous significance under HIPAA. What a covered entity describes in its NPP forms the outer envelope of how it can access, use and disclose PHI. Write the description too narrowly, and the covered entity forfeits the right to access, use and disclose PHI in ways not covered in the description, even if otherwise permitted under HIPAA, at least until the covered entity amends its NPP. Accordingly, we have encouraged covered entities to describe their possible access, use and disclosure of PHI in terms that are at least coextensive with their authority under state law and HIPAA.

Fundraising. First, the Final Rule now specifically requires that, before a covered entity may use or disclose PHI for fundraising purposes, it must state in its NPP that individuals may opt-out of receiving such communications. This is the required change.

However, as noted in the earlier fundraising discussion, the Final Rule also expands the types of PHI that may be used or disclosed for fundraising purposes, expands the covered entity's obligation to offer the opportunity to opt-out on all fundraising communications, and permits the opt-out to relate solely to the specific fundraising campaign or appeal for which a communication is made. While not required to amend the NPP for these changes, they are significant enough when implemented that we recommend addressing these three additional features in the fundraising discussion. This is particularly the case if the covered entity intends to limit the effect of opt-outs to only the specific fundraising campaign or appeal for which the communication was made, as opposed to giving general effect to an opt-out and not sending *any* further fundraising communications.

The Final Rule now specifically requires that, before a covered entity may use or disclose PHI for fundraising purposes, it must state in its NPP that individuals may opt-out of receiving such communications.

Public Health Activities. The Final Rule gives covered entities authority to disclose proof of immunization to schools, where immunization is a requirement for student enrollment. This disclosure authority is a new type of permitted public health disclosure. Since it is new and has its own description and conditions, it appears to require separate reference and description in the NPP, logically in an expanded description of permitted public health disclosures.

Deceased Individuals. The Final Rule makes two changes that should be addressed under the NPP provision dealing with deceased individuals. First, the Final Rule limits the period of time that the HIPAA privacy obligation follows the records of deceased individuals to 50 years following the death of the individual. Second, the Final Rule and preamble discussion make it expressly clear that a covered entity may continue to disclose PHI to family, friends and others who were involved in the individual's care or payment for care prior to death, as relevant to their involvement. Many NPPs are written too narrowly to accommodate this second change. We recommend that the NPP be edited to reference the 50-year privacy period. Also, covered entities should examine their existing text to see if edit on the second point is required under their current description of decedent rights.

Mandatory New NPP Content. The Final Rule specifically requires that four types of uses and disclosures that require the individual's authorization must be set forth in the NPP, if at all applicable to the covered entity's activities. These are:

- Psychotherapy Notes – the NPP must state that authorization is required for most uses and disclosures of psychotherapy notes. This will only affect covered entities that create or maintain psychotherapy notes.

- Marketing – the NPP must state that authorization will be required for marketing activity and, if the covered entity will receive financial remuneration from a third party in connection with marketing, the authorization must so inform the individual.

- Sale of PHI – the NPP must

state that any sale of PHI will require the authorization of the individual. Here again, the authorization must state that the disclosure will result in financial remuneration to the covered entity.

- Other uses and disclosures – the NPP must include a statement that uses and disclosures not described in the NPP require the individual's authorization. This statement, while highlighted in the Final Rule, probably already exists in most NPPs, but covered entities should check.

Request for Restriction. As is now well known, the HIPAA Rules have been amended to require covered entities to comply with a request for restriction by an individual not to disclose PHI to the person's health plan where the individual has paid for the episode of care in full. There are conditions and exceptions. The Final Rule requires that the NPP state that the individual may request, and the covered entity must comply with, such a request for restriction. This is now required content and should become part of the individual rights discussion of requests for restrictions.

Breach Notification. The Final Rule requires text informing individuals that the covered entity has a legal duty to notify the individual in the event there is a breach of the individual's unsecured PHI. Some commentators had requested that this part of the Notice go into detail regarding the covered entity's incident response and notification process. The Final Rule only requires a statement of the right to notification in the event of breach of unsecured PHI.

Expanded Access to PHI. Corresponding to the enhanced rights to request and direct distribution of PHI discussed elsewhere in this article, the NPP should now address the following new standards from the Final Rule:

- Electronic Access – If the entity maintains one or more designated record sets about the individual in electronic format and the individual requests an electronic copy, the covered entity is required to furnish the individual access in the electronic form or format requested, if readily producible.

- Distribution Instructions – The individual may direct the covered entity to "transmit" the individual's information to a designated third party, provided that the third party is clearly identified along with the mode of delivery.

These are enough of an expansion and change to existing access rights that we recommend they be included in the description of the individual's right to access.

Additional Requirements for Health Plans. There are several changes targeted specifically to health plans, one dealing with required content and the other with distribution.

- Most health plans (there is an exception for certain long-term care policies) that intend to use or disclose PHI for underwriting purposes must now include a specific statement in their NPP that they are prohibited by law from using genetic information for underwriting purposes.

- The Final Rule mandates two modes of distribution to health plan enrollees. If the health plan posts its NPP on its web site, it must prominently post the change (or its revised NPP) on the web site by the effective date of the change and provide the revised NPP, or information on how to obtain a copy, in its next *annual* mailing to individuals covered by the plan. If the health plan does not post its Notice on its web site, it must provide the revised NPP, or information on how to obtain a copy, to individuals covered by the plan within 60 days of the material revision.

Protections for Genetic Information

GINA prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts. In order to strengthen privacy protections for genetic information, GINA required the Secretary of HHS to clarify that genetic information is "health information" for purposes of the Privacy Rule and prohibit group health plans, health insurance issuers, and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

The Final Rule revises the definition of "health information" to include genetic information (e.g., information about genetic tests and family health history). In addition, the Final Rule prohibits all covered health plans that are covered entities under HIPAA,

including those to which GINA does not expressly apply (except issuers of long term care policies), from using or disclosing PHI that is genetic information (regardless of when the genetic information originated) for underwriting purposes. Thus, the use or disclosure of genetic information for underwriting purposes will now be considered a Privacy Rule violation. The prohibition is limited to health plans, and a health care provider may use or disclose genetic information for treatment purposes and as otherwise permitted under the Privacy Rule. Health plans will need to review and revise their policies and procedures and train appropriate staff members on the permissible uses of genetic information to ensure compliance with the Final Rule.

Miscellaneous Changes

There are other important changes of which covered entities and business associates must take note.

Immunizations. The exception for public health reporting at Section 512(b) has been amended to permit reporting immunization status to a school, with conditions. The conditions require: (i) PHI is limited to proof of immunization; (ii) the school must be required under state law to have proof of immunization prior to admitting the student; (iii) the report must be made to a school; and (iv) the covered entity must obtain and document some form of consent from a parent or guardian (or the individual, if an emancipated minor). OCR only went half way. Some form of consent is still required, but not a formal authorization.

Decedents. Under the Final Rule, the privacy restrictions only follow a decedent's records for 50 years following the individual's death. OCR also made a clarification in the Final Rule that will be useful. OCR states that the family, friends or others who played a role in an individual's care or payment for care before death may continue to have access to PHI in connection with their role. Thus, a family member or holder of power of attorney may continue to have access to PHI to file insurance claims, for example. Previously, the Rule and the commentary had suggested that only individuals who have recognized authority to deal with the affairs of decedents (for example, court-appointed executors or personal representatives) could have access. ■

Vickie B. Ahlers
Michael W. Chase
Alex M. "Kelly" Clarke

Upcoming Speaking Engagements

Several Baird Holm attorneys will be speaking at the upcoming Nebraska HFMA Annual Meeting. Andrew D. Kloeckner will speak on March 27. His topic is "Physician Financial Relationships- Stark, Anti-Kickback and Other Compliance Risks." John R. Holdenried will speak on March 28. His topic is "Physician Compensation: What's Fair and is it Commercially Reasonable?" ■

Health Care Group

Vickie Brady Ahlers
402.636.8230
vahlers@bairdholm.com

Michael W. Chase
402.636.8326
mchase@bairdholm.com

Alex (Kelly) M. Clarke
402.636.8204
kclarke@bairdholm.com

John R. Holdenried
402.636.8201
jholdenried@bairdholm.com

Andrew D. Kloeckner
402.636.8222
akloeckner@bairdholm.com

Julie A. Knutson
402.636.8327
jknutson@bairdholm.com

Barbara E. Person
402.636.8224
bperson@bairdholm.com

Whitney C. West
402.636.8353
wwest@bairdholm.com

All attorneys are admitted to practice in Nebraska and Iowa unless otherwise noted.

Health Law Advisory is intended for distribution to our clients and to others who have asked to be on our distribution list. If you wish to be removed from the distribution list, please notify healthupdate@bairdholm.com.

Baird Holm

1500 Woodmen Tower
1700 Farnam St
Omaha, NE 68102

402.344.0500
402.344.0588

www.bairdholm.com