BURR ALERT

New HIPAA Rules Issued: "Sweeping" Changes for Healthcare Providers and Business Associates

On January 17, 2013, the Department of Health and Human Services ("HHS") released its long-awaited final HIPAA rule, which significantly expands certain obligations for healthcare providers and their business associates (the "Final Rule"). The Final Rule, which was published in the Federal Register on January 25, 2013, has been described as "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented." In general, the Final Rule expands HIPAA obligations for business associates and their subcontractors, revises the requirements regarding the use and disclosure of patient information, expands patient rights, clarifies the content of Notice of Privacy Practices to be provided by healthcare providers, modifies the breach notification requirements, and expands enforcement provisions and penalties. The Final Rule is effective March 26, 2013. However, healthcare providers and business associates will have until September 23, 2013 (and in limited circumstances with respect to amending business associate agreements, until September 23, 2014) to achieve compliance with many of the new provisions. The Final Rule can be obtained at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

BUSINESS ASSOCIATES

Expanded Definition

Under HIPAA, a covered entity (*e.g.*, healthcare providers, health plans and health care clearinghouses) can disclose protected health information ("PHI") to a business associate, which is generally a person or entity that performs functions, activities or services on behalf of the covered entity that involve the use and/or disclosure of PHI. For a covered entity to use the services of a business associate, the covered entity must enter into a business associate agreement with the business associate. The business associate agreement obligates the business associate to comply with the HIPAA Security Rule and certain HIPAA Privacy Rule provisions.

The Final Rule specifically provides that the following entities will be considered business associates: (i) patient safety organizations, (ii) health information organizations, e-prescribing organizations or other persons that provide data transmission services to a covered entity and require routine access to PHI, and (iii) vendors of personal health records who access PHI on behalf of a covered entity. Further, by expanding the definition of business associate to a person or entity that creates, receives, *maintains*, or transmits PHI on behalf of a covered entity, data storage providers, even if they do not access a covered entity's PHI, are now considered business associates. However, an entity that is merely a conduit of PHI and does not require access (such as the U.S. Post Office or an internet service provider (ISP)) is not considered a business associate.

Subcontractors

The Final Rule also includes subcontractors in the definition of business associates. A "subcontractor" is defined as a person or entity to whom a business associate delegates a function, activity, or service. Accordingly, a subcontractor of a business associate that creates, receives, maintains or transmits PHI on behalf of the covered entity is now considered a business associate and must comply with HIPAA to the same extent as the business associate. For example, if a covered entity hires a business associate to handle PHI document and media shredding and the business associate retains a subcontractor to help with that service, then the subcontractor would be required to comply with the requirements of the HIPAA Security Rules (*e.g.*, with respect to the proper disposal of electronic PHI) and the HIPAA Privacy Rules (*e.g.*, with respect to limiting its uses and disclosures of PHI in accordance with its contract with the business associate.) It is the business associate's obligation, not the obligation of the covered entity, to make sure that a proper subcontractor business associate agreement is in place between the business associate and the subcontractor. Business associates and their subcontractors are directly liable for violations of their HIPAA obligations.

Compliance Obligations

The Final Rule clarifies that business associates and their subcontractors are required to comply with the HIPAA Security Rules and are responsible for limiting uses and disclosures of PHI as set forth in their business associate agreement and as required by the HIPAA Privacy Rule. In addition, business associates and their subcontractors are responsible for disclosing PHI when required by the Secretary of HHS, disclosing PHI to the covered entity or the patient in response to a request for an electronic copy of the patient's PHI, providing notice of a breach of unsecured PHI to the covered entity, and making reasonable efforts to comply with the minimum necessary requirements of the HIPAA Privacy Rule. However, not all HIPAA Privacy Rule requirements apply to business associates and their subcontractors. For example, business associates do not need a Notice of Privacy Practices and do not need to designate a privacy officer. However, business associates and their subcontractors are now directly liable for violations of their HIPAA obligations. Further, business associates are liable for failing to enter into a subcontractor business associate agreement with a subcontractor that creates or receives PHI for the covered entity.

The Final Rule grandfathers current business associate agreements for up to one year until September 23, 2014 if the agreements were in place prior to January 25, 2013, were fully HIPAA compliant and are not renewed or modified during the one year grandfather period. If a business associate agreement was not compliant as of January 25, 2013, is renewed or modified during the grandfathered period or if a subcontractor agreement with a business associate was not in place, then the compliance date for updating or entering into compliant agreements is September 23, 2013.

NEW USE AND DISCLOSURE REQUIREMENTS

Marketing

The HIPAA Privacy Rule requires covered entities to obtain a valid patient authorization before using or disclosing PHI to market a product or a service to the patient. Certain exceptions allow a covered entity to use PHI to market without an authorization, including communications to the patient for treatment purposes and communications to the patient to describe a health-related product or service provided by the covered entity.

The Final Rule provides that an authorization is needed for all treatment and health-related communications where the covered entity receives financial remuneration for making the communication from a third party whose product or service is being marketed. The term "financial remuneration" consists of direct or indirect payment to the covered entity. For example, if a hospital sent a letter to its patients notifying them of a new medical device, prior to the Final Rule an authorization would not be needed even if the letter was paid for by the medical device company. However, under the Final Rule, the hospital would need an authorization from each patient if the medical device company pays for the letter. An exception to this payment rule is allowed for subsidized refill reminders or communications about a currently prescribed drug or biological, as long as the payment is reasonable.

Fundraising

Prior to the Final Rule, a covered entity could only use or disclose demographic information and dates of service for fundraising purposes without a patient authorization. The Final Rule clarifies that demographic information includes the name, address, other contact information, age, gender, and date of birth of the patient. The Final Rule also allows a covered entity to use and disclose department of service information, treating physician information, outcome information, and health insurance status for fundraising purposes. Accordingly, covered entities can target select patients for fundraising activity, including patients who had positive outcomes. In addition, the Final Rule provides individuals greater opportunity to opt-out of future fundraising activity and provides covered entities greater flexibility to decide the method to allow an individual to opt-out (*e.g.*, toll-free number, email, etc.), as long as the method is clear and conspicuous and not unduly burdensome. The Final Rule also requires that a covered entity's Notice of Privacy Practices provide information on how an individual may opt-out of fundraising activity.

Sale of PHI

HIPAA has always prohibited the "sale" of PHI by a covered entity, unless an authorization was obtained from each subject individual. However, it was unclear whether a covered entity could receive payment for a disclosure of PHI permitted by the Privacy Rules. The Final Rule addresses this issue, and defines the "sale" of PHI to mean a disclosure of PHI by a covered entity or business associate, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. The Final Rule does not, however, prohibit the sale of PHI in connection with the transfer of ownership of

a covered entity where the purchaser is or will become a covered entity. Further, charging copy and transmittal fees for a disclosure of PHI in accordance with the Privacy Rules is not considered a "sale" of PHI and is therefore allowed.

Decedent Information

Prior to the Final Rule, a covered entity was required to apply the HIPAA protections regarding use and disclosure to decedent information regardless of how long ago the individual died. Further, a covered entity could not disclose PHI to a family member or friend involved in the patient's care after his/her demise unless the family member or friend was the decedent's legal representative as recognized by State law.

Under the Final Rule, a covered entity is only required to protect a decedent's PHI for 50 years following the individual's death. The Final Rule also allows covered entities to disclose a decedent's PHI to family members and others involved in the care or payment of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Student Immunization Records

Under the Final Rule, a covered entity has greater flexibility to disclose a student's immunization records to the student's school without authorization. Specifically, a covered entity can disclose immunization records to a school if such disclosure is required by law or upon the agreement of a parent or guardian. While it is recommended that a covered entity document a request for disclosure by a parent or guardian, the writing does not need to satisfy the specific requirements of a HIPAA authorization.

PATIENT RIGHTS

Right to Request Restrictions on Use and Disclosure

HIPAA requires covered entities to permit individuals to request that a covered entity restrict uses or disclosures of their PHI for treatment, payment and health care operations, as well as for disclosures to family members. Covered entities are not required to agree to such requests, but if they do, the covered entity must abide by the restriction. Under the Final Rule, a covered entity will be required to comply with a request of an individual to restrict disclosure of PHI to a health plan if the individual or a person on behalf of the individual, paid the covered entity in full for the health care item or service. Disclosures to Medicare and Medicaid would still need to be honored under the "required by law" requirements of the Privacy Rule. Covered entities will need to develop a method to flag or make a notation in the record with respect to PHI that has been restricted to ensure that such information is not inadvertently made accessible to the health plan for payment or other purposes.

Access of Individuals and Third-Parties to PHI

With limited exceptions, an individual has the right to review or obtain copies of their PHI maintained by a covered entity. If a covered entity maintains PHI in an electronic health record ("EHR"), the individual has the right to obtain a copy of the information in an electronic format and can direct the covered entity to transmit such copy to the individual's designee. The Final Rule expands an individual's right to obtain an electronic copy of their PHI stored in any electronic format, not just an EHR (*e.g.*, billing records, practice management software). The covered entity must provide the individual with access to the electronic information in the form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. If an individual requests access to his/her PHI by unencrypted email, the covered entity is permitted to do so, as long as the individual is advised of the risk of sending PHI without encryption.

If requested by an individual, the Final Rule requires that a covered entity transmit a copy of the individual's PHI to a third-party. The request must be made in writing, signed by the individual and clearly identify the designated person and where to send the copy of the PHI. A formal "HIPAA authorization" is no longer required for such disclosures. Covered entities are required to implement policies and procedures to verify the identity of any person who requests disclosure of PHI, as well as implement reasonable safeguards to protect the information that is used or disclosed. For example, reasonable safeguards would not require the covered entity to confirm that the individual provided the correct email address of the third-party, but would require reasonable procedures to ensure that the covered entity correctly enters the email address into its systems.

Under HIPAA, a covered entity must approve or deny, and if approved, provide access to PHI within 30 days of the request. In cases where the PHI is only accessible from an off-site location, the covered entity has 60 days to respond to the request. In extenuating circumstances, a covered entity may have a one-time 30 day extension. The Final Rule, however, removes the 60 day timeframe for off-site PHI, leaving covered entities only 30 days (with a possible 30 day extension) to provide access to all PHI. This change was due to the increasing use of EHR to store and maintain PHI.

BREACH NOTIFICATIONS

HIPAA requires that covered entities provide notification to affected individuals and the Secretary of HHS following the discovery of a breach of unsecured PHI. In some cases, HIPAA requires covered entities to also notify the media of breaches. The term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. Prior to the Final Rule, HIPAA allowed covered entity's to determine if the security or privacy of PHI was compromised based on a "harm standard". This standard provided that a breach of PHI would not have occurred unless the disclosure presented a significant risk of financial, reputational or other harm to the individual. Accordingly, a covered entity could analyze a breach of PHI and if it determined that the harm standard was not met then the disclosure of the breach was not required.

The Final Rule eliminates the "harm standard" and instead provides that an impermissible use or disclosure of PHI is presumed to be a breach and therefore notification is required unless a covered entity can demonstrate and document that there is a "low probability that the PHI has been compromised." A covered entity is required to consider and document four factors to determine whether the new "low probability" standard has been met:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

The Federal Register comments to the Final Rule provide substantial discussion of the analysis that a covered entity must undertake to determine if there is a low probability that the PHI has been compromised. It is clear from the discussion and examples provided in the Final Rule, that the Office of Civil Rights believes that it will be very difficult for a covered entity to demonstrate that a breach meets this new "low probability" standard. However, it is not clear that the new standard for determining a breach will result in a more objective analysis.

As stated above, when a breach of PHI occurs a covered entity has an obligation to report the breach to the affected individual, the Secretary of HHS and possibly the media. The obligation to report, and the time-frame for reporting, occurs once the covered entity "discovers" the breach. The Final Rule maintains the current breach notification requirements without modification, but provides clarification on when a breach is discovered, the time-frame for reporting a breach, methods of notification, and the content of the notice.

- Under HIPAA a breach is discovered once an employee, officer, or other agent of the covered entity "knows or should reasonably have known of the breach". The comments to the Final Rule provide that a covered entity must excise reasonable diligence to determine a breach, and that such determination is generally a factual one, since what is reasonable depends on the circumstances. Factors to be considered include whether a covered entity took reasonable steps to learn of the breaches and whether there were indications of breaches that a person seeking to satisfy HIPAA would have investigated under similar circumstances.

- HIPAA requires covered entities to notify individuals of a breach within 60 days from the discovery of the breach, except if law enforcement requests a delay. The Final Rule makes it clear that the time period begins to run when the incident becomes known, not when it is determined that a breach as defined by HIPAA has occurred.

- The content of any breach notification is provided for in the HIPAA rules, and generally requires: (i) a brief description of the breach, (ii) a description of the type of PHI

involved in the breach, (iii) any steps the individual should take to mitigate harm from the breach, and (iv) a description of what the covered entity is doing to investigate and mitigate the breach, and (v) contact procedures for the individual to ask questions or obtain more information. The Final Rule makes it clear that a notice has not been given if undeliverable, but does allow notification by email in certain circumstances. Further, if more than 10 notices are returned and the covered entity is unable to identify correct addresses or contact information within the 60 day notice period, the covered entity is required to post notices on its website.

UPDATES TO NOTICE OF PRIVACY PRACTICES

HIPAA requires that covered entities distribute a Notice of Privacy Practices to patients describing the uses and disclosures of PHI a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to PHI and the individual's rights concerning PHI. Covered entities will need to update their Notice of Privacy Practices to address the changes in the Final Rule. (If a covered entity did not update their Notice of Privacy Practices after the 2009 amendments to HIPAA brought about by the so-called "HITECH" Act, any updates will also need to address the HITECH changes.) For example, Notice of Privacy Practices will need to address the prohibition on the sale of PHI, new opt-out requirements for fundraising, marketing limitations, an individual's right to restrict access to PHI to a health plan, and new HIPAA breach notification requirements. The Notice must also include a statement that a HIPAA authorization will be required for uses and disclosures not described in the Notice of Privacy Practices.

THE ENFORCEMENT RULE

As it relates to the enforcement provisions, the Final Rule clarifies the categories of violations under HIPAA and factors used to determine civil money penalties. Significantly, the Final Rule also imposes civil money penalties directly on business associates and their subcontractors and provides for liability of covered entities and business associates for violations caused by their agents. Finally, the Final Rule requires (instead of permitting) HHS to conduct compliance reviews and investigations for certain HIPAA violations and no longer requires HHS to first attempt informal resolution of a violation prior to imposing civil money penalties.

Civil Money Penalties

The Final Rule retains the tiered civil money penalty structure that was implemented in the Interim Final Rule. As a refresher, the tiered system uses increasing penalties based on increasing levels of culpability:

- For a violation in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision, an amount not less than $100 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to "reasonable cause" and not to willful neglect, an amount not less than $1,000 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to willful neglect but was corrected during the 30–day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, an amount not less than $10,000 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30–day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, an amount not less than $50,000 for each violation.

The Final Rule clarifies the "state of mind" requirement required for application of the second tier, which provides that a violation occurred when it is established that the violation was due to reasonable cause and not to willful neglect. "Reasonable cause" is now defined as an act or omission in which the covered entity or business associate knew or by reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but which the covered entity or business associate did not act with willful neglect.

The Final Rule also lists numerous factors that HHS considers in determining the amount of a civil money penalty to impose for a HIPAA violation. The factors include (1) the nature and extent of the violation (including the number of individuals affected and the time period), (2) the nature and extent of the harm resulting from the violation (including whether the violation caused physical harm, financial harm or harm to the individual's reputation), (3) the covered entity or business associate's history of prior compliance with HIPAA, and (4) the financial condition of the covered entity or business associate (including the size of the entity, whether the civil money penalty would jeopardize the ability to continue to provide healthcare and whether the entity had financial difficulties that affected its ability to comply).

Direct Liability for Business Associates and Their Subcontractors

As mentioned above, many of the provisions of HIPAA and the HITECH Act now apply directly to business associates and their subcontractors in substantially the same manner as they apply to covered entities. Consequently, business associates and their subcontractors are subject to civil money penalties for HIPAA violations as mentioned in the preceding section.

Liability for the Acts of Agents

The Final Rule also extends liability to covered entities and business associates when a HIPAA violation is caused by one of their agents. Previously, a covered entity would not be liable for a HIPAA violation caused by an agent as long as the covered entity had met business associate agreement requirements, did not know the business associate was in violation of the

agreement and did not fail to act as required by HIPAA if it was aware of a pattern or practice of violations by the agent. Now, covered entities and business associates can be held liable for the acts of their agents acting within the scope of the agency, regardless of whether the covered entity or business associate did no wrong themselves. HHS acknowledges that whether or not a business associate is an agent of a covered entity will be fact-specific, taking into account the terms of the business associate agreement and the totality of the circumstances involved in the relationship. The biggest factor in determining liability for the acts of agents will be the right or authority of the principal (*e.g.* the covered entity or business associate) to control the conduct of the agent. Other factors HHS will consider include (1) the time, place and purpose of the business associate's (or subcontractor's) conduct, (2) whether the agent engaged in a course of conduct subject to the principal's control, (3) whether the agent engaged in conduct that is of the type a business associate will commonly engage in to accomplish the services provided to the covered entity, and (3) whether the covered entity reasonably expected its business associate to engage in the conduct in question.

Compliance Reviews and Investigations

Previously, HHS had the discretion to investigate complaints and to conduct compliance reviews. Under the Final Rule, HHS is now required to conduct a complaint investigation or compliance review where facts indicate a possible violation due to willful neglect. Where willful neglect is not indicated, HHS still retains discretion to decide whether to conduct a compliance review or complaint investigation.

Attempt at Formal Settlement

The previous HIPAA rules also required HHS to first attempt to resolve noncompliance by informal means such as settlement agreements with covered entities. The Final Rule now provides HHS with discretion to attempt settlement prior to seeking civil money penalties. Consequently, HHS may pursue civil money penalties directly without attempting informal resolution efforts.

The enforcement provisions under the Final Rule are effective March 26, 2013, and are not subject to the 180 extension (to September 23, 2013) that applies to most other provisions of the Final Rule.

ACTION ITEMS

In response to the passage of the Final Rule, and the increased HIPAA enforcement activity, covered entities should undertake the following steps:

1. Perform a "gap" analysis to determine what changes are needed to existing HIPAA policies, procedures and forms to address the Final Rule provisions, as well as any changes to address current HIPAA Privacy Rule, HIPAA Security Rule and HITECH Act requirements.

2. Revise existing HIPAA policies, procedures and forms as appropriate. It will be important to ensure that the policies and procedures accurately reflect the operations of the covered entity and that the covered entity has taken the necessary steps to ensure compliance.

3. Update and revise existing business associate agreements to address the Final Rule provisions and obtain new business associate agreements as needed (*e.g.*, for data storage providers, even if they do not access PHI).

4. Notify business associates of their obligation to comply with the HIPAA Security Rule and certain parts of the HIPAA Privacy Rule, including the obligation to conduct a Security Rule analysis. Also, notify business associates of their obligation to obtain appropriate HIPAA agreements with their subcontractors who have access to PHI.

5. Amend Notices of Privacy Practices to address the Final Rule provisions. The new Notices should be distributed and posted as required by HIPAA.

6. Train workforce members on the new HIPAA requirements and obligations.

7. Implement, as possible, encryption technology for PHI (especially on laptops and other portable devices) to minimize the risk of having to disclose a breach of PHI.

If you have any questions or if you would like additional information on this topic, please contact any Burr & Forman attorney listed below. Also, please visit our website at www.burr.com where you can access information on additional health law topics and learn more about the firm.

HOWARD BOGARD
Partner ~ Birmingham
(205) 458-5416
hbogard@burr.com

KELLI FLEMING
Partner ~ Birmingham
(205) 458-5429
kfleming@burr.com

C. LOGAN HINKLE
Partner ~ Birmingham
(205) 458-5154
lhinkle@burr.com

JAMES HOOVER
Partner ~ Birmingham
(205) 458-5111
jhoover@burr.com

DEBRA MACKEY
Counsel ~ Birmingham
(205) 458-5484
dmackey@burr.com