SUMMER/FALL 2013

HALL RENDER'S PRACTICALHEALTH

HIPAA Goes HITECH: Practical Application of the Final Rule

The Final Rule makes significant changes to the HIPAA Privacy and Security Rules, requiring covered entities and business associates to take several actions by the compliance deadline, September 23, 2013.

BACKGROUND

On January 25, 2013, the Department of Health and Human Services issued its Omnibus Final Rule ("Final Rule") under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. The Final Rule makes significant changes to the HIPAA Privacy and Security Rules, requiring covered entities and business associates to take several actions by the compliance deadline, September 23, 2013. A copy of the Final Rule may be accessed at http://tinyurl.com/HITECHfinalrule.

KEY CHANGES AND PRACTICAL APPLICATION

Business Associates. Business associates are now directly liable for compliance with the Security Rule and many Privacy Rule requirements. The Final Rule expands the definition of "business associate" by listing several types of entities and by specifying that maintaining and transmitting protected health information ("PHI") on behalf of a covered entity triggers business associate-status.

These changes present a prime opportunity for covered entities to review their vendors and identify their business associates. When updating the list of business associates, a covered entity should include patient safety organizations, data transmission organizations, vendors of personal health records and data storage vendors. The covered entity may, however, leave out any treatment arrangements, business associate subcontractors and entities within the same organized health care arrangement.

Business Associate Agreements. Covered entities should review their current business associate agreements to determine if their business associate agreements already meet the Final Rule requirements, qualify for the "grandfathering" compliance date of September 22, 2014 or need to be amended prior to the September 23, 2013 compliance deadline. Business associate templates should be updated for future agreements and renewals. CONTINUED ON PAGE 2

HALL RENDER
KILLIAN HEATH & LYMAN
hallrender.com

HIPAA Goes HITECH: Practical Application of the Final Rule
(Continued)

Breach Notification. Under the Final Rule, "breach" means the acquisition, access, use or disclosure of unsecured PHI not permitted by the Privacy Rule unless there is a low probability the PHI has been compromised based on a risk assessment. Under the prior Interim Final Breach Notification Rule, the standard triggering breach notification was whether the incident created a significant risk of harm to individuals.

Fundraising. The Final Rule expanded the types of PHI covered entities may use for fundraising activities. In addition to demographic information, health insurance status and dates of service, covered entities may now also use date of birth, department of service, treating physician and outcome information.

The Final Rule also imposed a new requirement that the opt-out provision in fundraising communications be made in a clear and conspicuous manner. The opt-out process may not impose undue burden on individuals. Reasonable effort is no longer enough; covered entities must comply with opt-outs and permit an opt-back-in if requested. The Final Rule clarifies that a fundraising communication program may be designed to apply to all fundraising activities or individualized by campaign.

Marketing. The Final Rule made several changes to the HIPAA marketing rules, specifying when PHI may be used to make communications about products or services that encourage the recipient to purchase or use the products or services. As a general rule, using PHI for marketing purposes is prohibited unless there is a patient authorization or an exception applies and only permitted remuneration is exchanged.

Sale of Protected Health Information. The Final Rule created a new prohibition: PHI may not be exchanged for remuneration unless permitted by a patient authorization or under a specified exception, such as for public health activities, treatment purposes and business associate services.

Research. The Final Rule reversed the prior rule that research authorizations may not be combined with other written permissions. Now, research authorizations may be combined with authorizations for purposes such as research repositories and databases. Such "compound authorizations" must clearly distinguish between conditioned and non-conditioned research components and permit the individual to opt-in to the unconditioned components. The Final Rule also clarified that research authorizations may now be used for "future" research studies.

Right of Access. The Final Rule expanded the patient right of access to include electronic copies of medical records be provided in the electronic form and format specified by the patient. Patients also have the right to have an electronic copy sent directly to another person or entity designated by the individual. Covered entities may impose reasonable, cost-based fees for e-copies, which may include portable media costs, postage and labor costs. The Final Rule removed the additional 30-day period covered entities had to respond to access requests for records stored off-site.

Right to Request Restrictions. The Final Rule requires covered entities to grant a patient's request that a claim not be submitted to the patient's health plan for services the patient paid for out-of-pocket and in-full. Covered entities may still deny other types of restriction requests.

Decedents. The Final Rule clarified that covered entities may continue to disclose the same type and scope of PHI to involved family and friends after a patient's death as when the patient was living. Under the Final Rule, PHI is no longer subject to HIPAA after the patient has been deceased 50 years. There is no HIPAA requirement to maintain or disclose this type of PHI. Covered entities should also note that more stringent state laws continue to apply and may trump this new rule.

Immunizations. The Final Rule permits covered entities to disclose immunization records to a school upon the request of a patient or parent in lieu of a HIPAA authorization. The covered entity must document this request.

Notice of Privacy Practices. Covered entities must update their notices of privacy practices ("Notices") to reflect changes imposed by the Final Rule. The revised Notice must be posted on the covered entity's website and in the lobby. New patients must be provided with a copy of the revised Notice. Covered entities do not have to redistribute the Notice to returning patients who received the prior Notice, but they have to make the revised Notice available upon request.

The Final Rule requires covered entities to update their business associate agreements, implement changes to their policies and procedures, revise and repost their Notices and reeducate their workforces. Business associates must also update their business associate agreements, implement new policies and procedures and educate their workforces.

All of these compliance actions are required by September 23, 2013. For more information on the Final Rule, please visit our website at **www.hallrender.com/hipaa** or contact your Hall Render attorney. ■

HIPAA Enforcement: Past, Present and Future

In recent years, the number and scope of HIPAA enforcement activities by OCR has increased dramatically. This increase in enforcement is in part due to new rules introduced by HITECH. HITECH expanded HIPAA enforcement by providing higher penalties; broadening the range of potential targets, such as business associates; and increasing enforcement authority of state attorneys general. While the full impact of the new privacy and security rules under HITECH have yet to be seen, providers and hospitals can look to OCR's past HIPAA enforcement activity as an indicator of what may lie ahead.

While active enforcement did not regularly occur in the first several years after the HIPAA Privacy Rule and Security Rule went into effect, in recent years, that has changed. To date, OCR has entered into fifteen resolution agreements: one each in 2008 and 2009, two in 2010, five in 2012 and five already through the middle of 2013. These resolution agreements have involved financial penalties ranging from $50,000 to $4.3 million. The pattern of HIPAA enforcement actions seems to highlight teachable moments that shed light on particular areas of vulnerability. These pose high risks of breaches, but OCR has investigated many different breach issues and types and sizes of covered entities.

OCR used these enforcement actions to send the message that all covered entities are expected to comply with HIPAA at all times. These settlements will help to fund continued HIPAA enforcement efforts by OCR. ■

Breach Notification: Next Steps once a Potential Breach Has Been Identified

Even with the most comprehensive compliance programs and safeguards in place, it is nearly impossible to stop all breaches from occurring; therefore, it is important to have a comprehensive plan for dealing with a potential breach. The following are the steps a covered entity should take once a potential breach has been identified.

1. INVESTIGATE

Conduct an investigation to determine whether a breach occurred, what type of information it involved and how many individuals are involved. If a business associate is involved, the covered entity should obtain as much information from the business associate as possible.

2. PREVENT FURTHER MISUSE

Take all available steps to prevent further misuse or disclosure of the information and to mitigate any potential harm that could result from the breach.

3. DETERMINE NOTIFICATION

Determine whether notification to individuals and HHS is required. As of September 23, 2013, Privacy Rule violations involving unsecured PHI will require notification unless the covered entity can document a low probability that the information will be compromised.

4. DETERMINE TIMING

Determine the timing for notification to HHS. For breaches affecting fewer than 500 individuals, notification must be made annually by March 1. For breaches affecting 500 or more individuals, notice to HHS must be made at the time notice to individuals is sent.

5. NOTIFY MEDIA

Provide notice to prominent media outlets if the breach affects 500 or more individuals or if there is insufficient contact information for 10 or more individuals.

6. DEVELOP COMMUNICATIONS PLAN

Develop a communications plan so that covered entity staff who receive telephone calls or questions from patients regarding the incident can deliver an accurate, consistent message. Often times, this will necessitate the use of a dedicated call center.

7. DOCUMENT INVESTIGATION

Document the investigation and all steps taken in response. Documentation is essential in any follow-up investigation by HHS.

Covered entities should work closely with legal counsel to ensure that all necessary steps are timely and effectively performed.

Physician Contracting: An Ounce of Prevention Is Worth a Ton of Cure.

7 BEST PRACTICES TO MAINTAIN COMPLIANCE IN TODAY'S REGULATORY ENVIRONMENT.

In 2012, the United States government won or negotiated over $3 billion in health care fraud and abuse judgments and settlements.

Some of the most significant penalties were assessed to health care systems that failed to adequately monitor their physician arrangements, which proved to be costly for all involved. Often the simplest contract terms to monitor received the least attention (e.g., expiration dates) and resulted in the costliest penalties. Many systems lack a formal process that ensures regular contract reviews. Many more lack automated tools to help them with the work involved.

So in this era of ever-increasing hospital and physician integrations, coupled with a highly technical and complicated regulatory environment, what best practices can we offer to those who want to avoid the pain that comes from running afoul of the law and the disproportionate penalties that follow?

7 BEST PRACTICES FOR PHYSICIAN CONTRACTING

1. **Maintain a written protocol that describes the process applicable to all physician financial arrangements.** It should address the basics, including signature authority, the pre-execution review process, required terms, the fair market value process, the periodic review process and the responsible internal contract manager or business lead.

2. **Invest in standard contract templates for common contracts such as medical director arrangements, on-call agreements and leases for office space.** Templates help ensure required elements of Stark exception or AKS safe harbor are included in the terms of the contract (e.g., time sheet requirement for medical directors). Templates do not, however, eliminate the need for careful review and oversight from legal counsel.

3. **Verify the need for services.** Commercial reasonableness is an explicit requirement in most of the applicable Stark exceptions and AKS safe harbors. Do you have a sound business or clinical purpose for entering into the arrangement with the physician? Be sure to define the need for the service in the contract.

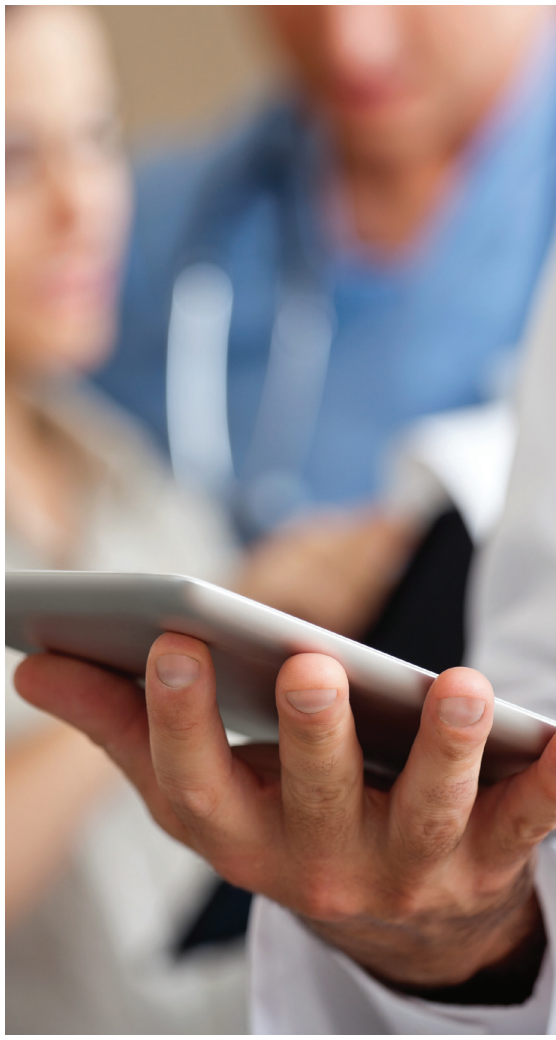
4. **Define the specific services a physician is to provide, or in the case of office space leases, describe the space to be leased to the physician.** Being detailed helps demonstrate the commercial reasonableness and fair market value of the arrangement and avoid common problems created by including vague phrases like, "physician agrees to provide medical services to hospital patients."

5. **Invest in a contract management system.** An effective contract management system is imperative. The system should advise the provider of deadlines, necessary changes and other events when Stark compliance could become in jeopardy and link the system with accounts payable (no payment without verification of a written contract).

6. **Conduct regular contract reviews.** Confirm that the contract is not expired and that services are still necessary. Review accounts payable data and match to contract terms.

7. **Self-disclosure.** If after a full internal investigation you find problems, contact legal counsel to determine the appropriate process for reporting actual or potential violations. Confirm that there are no other problematic arrangements to avoid multiple disclosures. It is critical to also report any problems that resulted in government overpayments. ■

For more information, contact Jerry Hallett at 317.429.3902 or jhallett@ntracts.com.



Quarterly Check-Up

Health Care Daily Deals: Gaining New Patients or Inviting Legal Headaches? "Daily deal" websites are gaining popularity among health care providers for the ability to attract attention from new and existing patients. Health care providers must be aware that the offering of discounted services may violate various federal and state laws, as well as rules and regulations. **http://tinyurl.com/healthcaredeals**

New Proposed Regulations on Code Section 501(r) Released. The IRS released a new round of proposed regulations that expand upon the requirements of Code Section 501(r) applicable to tax-exempt hospital organizations. **http://tinyurl.com/501RegsReleased**

HHS Announces $400,000 HIPAA Enforcement Action. HHS announced a settlement with a state university arising out of alleged HIPAA violations discovered when the university self-reported a breach of unsecured electronic PHI for patients at one of its medicine clinics. **http://tinyurl.com/EnforcementAction**

IRS Releases New Required Form for TEB VCAP Submissions. On March 8, 2013, the IRS released Form 14429, Tax Exempt Bonds Voluntary Closing Agreement Program Request. The purpose of the new form is to assist issuers in organizing submission requests and to ensure that their submissions are complete and comply with necessary requirements. **http://tinyurl.com/TEB-VCAP-Form**

Unpaid Medical Intern Is Not an Employee Under the Health Care Worker Protection Act. The Wisconsin Court of Appeals affirmed a decision by the Labor and Industry Review Commission that an unpaid intern is not an employee for purposes of Wisconsin's Health Care Worker Protection Act.
http://tinyurl.com/MedInternEmployment

U.S. Customs and Border Protection Begins Implementation of Automated Form I-94. On April 30, 2013, U.S. Customs and Border Protection began implementing an automated version of Form I-94, Arrival/Departure Record, at air and sea ports of entry. Form I-94 provides foreign travelers with evidence that they have been lawfully admitted to the United States, which is necessary for employment authorization. **http://tinyurl.com/AutomatedFormI94**

Significant Changes to DSH Under Proposed 2014 IPPS Rules. On April 26, 2013, CMS released proposed rules for the reduction in DSH payments to hospitals. If the proposed rule is implemented, it will adversely affect hospitals in states that have opted out of the Medicaid expansion.
http://tinyurl.com/DSH-IPPS-Rules

OIG Report Shows Many Co-Located LTCHs Fail to Notify of Co-Located Status; LTCHs Face Potential Overpayment Risk. The OIG report shows that a significant number of Long-Term Care Hospitals ("LTCHs") that are co-located with skilled nursing facilities or acute care hospitals are failing to notify their Medicare Administrative Contractors or fiscal intermediaries of their co-located status. **http://tinyurl.com/LTCH-OverpaymentRisk**

Final Sunshine Rule Requires Reporting of Physician Ownership in GPOs and Health Products Manufacturers. The Final Sunshine Rule, released on February 1, 2013, requires drug, biological and medical device manufacturers, as well as group purchasing organizations, to annually disclose direct and indirect ownership and investment interests held by physicians and their immediate family members. The Sunshine Act also requires that group purchasing organizations disclose payments and transfers of value made to physician owners and investors. **http://tinyurl.com/SunshineRuleGPOs**

Hospital Value-Based Purchasing Metrics for Fiscal Year 2015 Are Underway. The Value-Based Purchasing FY 2015 Total Performance Score performance periods are currently underway. The Outcomes category's performance period ended June 30, 2013. All other categories' performance periods end on December 21, 2013.
http://tinyurl.com/Purchasing-Metrics

OIG Releases Physician-Owned Entity Special Fraud Alert. The OIG released a special fraud alert regarding physician-owned distributorships that focused on the characteristics of the distributorships that the OIG believes pose the greatest risks of fraud and abuse, as well as dangers to patient safety.
http://tinyurl.com/OIG-Fraud-Alert-Released

Off-Label Use of Medical Products: Warranty and Indemnification Considerations in Purchase Agreements. Suppliers of medical products often attempt to carve out off-label use in warranties and indemnification provisions of product purchase agreements with customers. There are several points that purchasing entities should consider with regard to off-label use when negotiating purchase agreements for medical products. **http://tinyurl.com/Off-Label-Use**

OIG Issues Updated Self-Disclosure Protocol. On April 17, 2013, the OIG issued an updated version of its Self-Disclosure Protocol ("Protocol"). The Protocol includes key improvements that should make it a more attractive tool for disclosing parties to resolve instances of potential fraud involving federal health care programs. **http://tinyurl.com/OIG-Updated-Protocol** ■

VISIT HALL RENDER'S HIPAA GOES HITECH RESOURCE at **hallrender.com/hipaa** to view the latest on compliance and security news, as well as resources and insight from our attorneys.

ABOUT HALL RENDER

With more than 160 attorneys, Hall Render partners with clients to direct them through the ever-changing business landscape of today's health care industry. Health law is our business.

CONTRIBUTING AUTHORS

ELIZABETH CALLAHAN-MORRIS

Elizabeth focuses her practice in the areas of HIPAA privacy and security, patient care issues and corporate compliance. She advises hospitals and other health care organizations on all aspects of compliance programs, including conducting compliance programs assessments, developing policies and audit work plans, training and education, conducting internal investigations, responding to government investigations and arranging voluntary self-reporting. She is proficient in state and federal patient confidentiality laws, data breach reporting and Office for Civil Rights HIPAA investigations. Elizabeth is a frequent speaker on HIPAA and corporate compliance topics at the local and national levels.

MARK SWEARINGEN

Mark coordinates the firm's HIPAA practice and provides counsel on health information privacy and security matters such as breach response and notification and the creation, use, disclosure, retention and destruction of medical records and other health information. His counsel to clients also includes a variety of health care topics related to regulatory compliance, physician and clinical services contracting, risk management and Independent Review Organization services. He has provided such services to a broad spectrum of health system, hospital, physician practice, diagnostic imaging center, ambulatory surgical center and long-term care facility clients. Mark has spoken and written nationally and regionally on numerous topics, including antitrust, electronic medical records and health information privacy and confidentiality.

ALYSSA CONLEY JAMES, Law Clerk, also contributing.

MATTHEW DECKER, Law Clerk, also contributing.

KIMBERLY REESE, Law Clerk, also contributing.

HALL RENDER IS ON TWITTER

Keep up with the latest health law news and insights by following **@hallrender**.

HALL RENDER
KILLIAN HEATH & LYMAN
hallrender.com