Independent Insurance Agents & Brokers of Louisiana
9818 Bluebonnet Boulevard
Baton Rouge, Louisiana 70810
www.IIABL.com
(225) 819-8007

Technical Advisory

TA 309 **August 13, 2013**

Subject: **HIPAA Omnibus Rule will have Big Impact on "Business Associates"**

Background: This final rule goes into effect on September 23 and will now require HHS to conduct periodic audits of Business Associates as well as Covered Entities for compliance with HIPAA and authorizes HHS, as well as state attorney generals, to impose significant fines directly on Business Associates which are not in compliance.

ACT's (Agents Council for Technology) HIPAA Work Group prepared this information to raise agent awareness about the final HIPAA Omnibus Rule, provide guidance on the key compliance measures they should take and to reference a number of resources agencies can use to help them comply.

The article is relevant to all agencies – even if they do not sell health insurance – because it provides security measures they should take and references resources they can use to formulate their general security plans and procedures, in order to be compliant with the federal and state privacy and data breach notification laws that do apply to them (because of the PII (personally identifiable information) that they do handle).

The HIPAA Omnibus Rule also requires independent agencies which are Business Associates to obtain Business Associate agreements by September 23 from any vendors who manage online systems for the agency, if the agency stores PHI (Protected Health Information) on those systems (such as on health insurance applications).

Main Points: The HIPAA Omnibus Rule goes into effect on September 23, 2013 and promises to bring a much higher degree of enforcement attention on independent agencies and brokerages which are "Business Associates" under HIPAA. HHS is now required to conduct periodic audits of both Covered Entities and Business Associates for compliance with HIPAA, and the state attorney generals are authorized as well to bring HIPAA related actions. Note there is no need for there to have been a breach of Protected Health Information ("PHI") to trigger such an audit and enforcement action. It is a matter as to whether the Business Associate or Covered Entity has properly implemented the HIPAA compliance requirements.

Who is a Business Associate under HIPAA?

Agencies which sell ANY health insurance products (medical, dental, vision, long term care, Medicare supplements) for companies like Blue Cross/Blue Shield, Humana, Aetna, Principal, Delta Dental, etc. are likely to be Business Associates and their agent agreements will include provisions that require them as Business Associates to comply fully with the HIPAA Security Rule, as well as with the portions of the HIPAA Privacy and Data Breach Rules that are applicable to them.

The 2009 HITECH Act made these HIPAA Rules directly applicable to Business Associates, rather than just via contract with Covered Entities and rendered Business Associates subject to the same civil and criminal penalties and fines that Covered Entities have experienced for failing their audits in recent years.

A "Business Associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity. For it to be PHI, the health information has to include elements that can be used to identify the individual to which the information belongs. "Covered Entities" include health plans, health care clearinghouses and certain types of health providers.

HIPAA does not apply to medical information relating to life insurance, worker's compensation, auto insurance or other casualty insurance, however, these types of medical information are also highly sensitive and need to be carefully secured by the agency. These other types of medical information are typically protected by other federal and state privacy and data breach notification laws.

Even if an agency is not subject to HIPAA, it will find the resources mentioned in this article to be helpful tools in doing its risk analysis and formulating its security plan and procedures, so that it is compliant with the Gramm-Leach-Bliley Act (GLBA) and other federal and state privacy and data breach notification laws with regard to the protected personally identifiable information ("PII") that it does handle.

Impact of HIPAA Omnibus Rule on Business Associates

The HIPAA Omnibus Rule, effective on September 23, 2013, gives full force and effect to the significant new HIPAA Privacy and Security compliance requirements contained in the 2009 HITECH Act, which amended HIPAA. Here is what the rule means for Business Associates:

- Business Associates are now subject to the same comprehensive Privacy and Security Rule requirements as Covered Entities, as well as to relevant sections of the HIPAA/HITECH Breach Notification Rule. Below we reference an online tool California has developed to assist organizations in complying with the many requirements of the Security Rule.
- HHS and state attorney generals may now impose substantial fines against Business Associates who do not comply with HIPAA/HITECH. Where there is HIPAA "Willful Neglect" – "conscious, intentional failure or reckless

indifference to the obligation to comply" – HHS is obligated to investigate violations and the potential penalties become very severe.

- Business Associates are required to execute Business Associate Agreements with any subcontractors which are given access to their PHI. For example, if the Business Associate stores PHI on an online system managed by a vendor, then the Business Associate will need to execute such an agreement with the vendor. HSS provides sample Business Associate Agreement provisions.

- See "Health Care Providers, HIPAA Privacy and Security Compliance and the Effects of the 2013 HIPAA Omnibus Rule," by Paul Hales, for an excellent overview of the many additional changes included in the new Omnibus Rule.

Key Areas of Emphasis for Business Associates

According to Paul Hales, HHS has focused its enforcement actions on covered entities to-date and has cited them for "inadequate or no risk analysis and risk management programs, inadequate or no contingency plans [to protect the PHI in the event of loss or disaster], inadequate and incomplete policies, procedures, documentation and ineffective workforce training." *Note there does not need to be a data breach to trigger an enforcement action*; however, if there is a data breach, you can bet that HHS and state attorney generals will be looking at all of these areas.

The HIPAA Omnibus Rule, effective September 23, provides for an expansion of these enforcement actions to Business Associates. HHS's past actions provide a good roadmap for the kinds of things they will be looking for from Business Associates as well. We recommend that Business Associates:

- Conduct a Risk Analysis, which requires the organization to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the entity."

- Then implement a HIPAA/HITECH Risk Management Program, which incorporates "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."

- Complete compliance gap assessments to ensure that your Risk Management Program has addressed all applicable sections of the rules. The Security Rule explicitly requires this gap assessment, called an Evaluation (45 CFR §164.308(a)(8)), and its simply good business practice to perform the same type of compliance gap assessment for the Privacy and Breach Notification rules.

- Develop policies and procedures to implement the HIPAA/HITECH Risk Management Program and cover all applicable standards and implementation specifications in the Privacy, Security and Breach Notification rules.

- Train employees on the policies and procedures at least annually and clearly define the disciplinary consequences to employees if they fail to adhere to the agency's security policies. Maintain accurate records of the training that has been performed.

- Document, document, document, so that you can demonstrate that you have taken all of these steps.

- Execute a Business Associate agreement with any vendor that has access to your PHI by September 23.

Tools to help Business Associates Comply

Hopefully, many agencies will be able to build upon the security plan and procedures that they have already established. In addition, HHS has created the seven part HIPAA Security Series which outlines the administrative, physical and technical safeguards that the HIPAA Security Rule requires, coupled with the requirements relating to the organization, policies and procedures, documentation, conducting a risk analysis and creating a risk management plan.

California has created a great resource for Business Associates to use – HIPAA Security Rule Toolkit – to help them comply with the HIPAA Security Rule. It provides a checklist of all of the requirements and provides a field for the organization to document what the entity has done to comply with each requirement. Note that the requirements include creating a continuity plan, so that PHI is preserved in the event of a disaster or potential loss of the data.

Cornell University Law School provides another excellent summary of the required HIPAA administrative, physical and technical safeguards which apply equally to Covered Entities and Business Associates. (Click "PREV & NEXT" on the tool to move among the different safeguards.)

Some Additional Key Areas for Emphasis

As the agency develops its Risk Management Program, here are some important areas to emphasize:

- Identify and document where all the PHI "lives" in your organization –- whether paper, electronic or orally communicated.
- Keep the HIPAA Minimum Necessary Requirement of the Privacy Rule in mind, which requires the entity to limit access to PHI to only those employees who need to see the information and to limit disclosure of PHI to the minimum necessary to accomplish the purpose.
- Minimize the amount of Protected Health Information (PHI) that the agency sees or retains to the maximum extent possible. If PHI must be retained in your system, encrypt the data or put it in a password protected PDF. Check with your vendor to see if it is already providing "encrypted data at rest" – which would be a big plus.
- Always use secure email when transporting PHI by email.
- Make sure back ups of PHI are encrypted and kept in a safe and secure place.
- Keep PHI off of laptops, tablets, smart phones, thumb drives, etc. where there is a high risk of loss or theft. Develop and implement your Bring Your Own Device ("BYOD") policies and procedures which should include your mobile device management plan. (See the ACT article, "Bring Your Own Device" Opportunities & Risks.)
- Regular *monitoring* of systems and traffic for unusual activity and *auditing* employees for adherence to the agency's security procedures are critical to HIPAA compliance.
- Document the process you will follow if there is a breach of PHI in your Risk Management Program, making sure the process complies with the Breach Notification Rule, which requires Business Associates to notify the Covered

Entity without unreasonable delay and in any event, no later than within 60 days. Review your agency agreements to see the time period your insurers require for notifying them of breaches – which is likely to be much shorter. The Covered Entity then has obligations to notify the affected individuals, HHS, and the local media (if the breach affects 500 or more people).

Additional Resources

Because of the complexities of HIPAA, agencies may want to engage a firm to assist them with their risk analysis and the development of their HIPAA compliance program. Some of the firms offering independent agencies and other businesses with consulting, tools and sample policies and procedures for HIPAA compliance are:

Bob Chaput, Clearwater Compliance, LLC, bob.chaput@ClearwaterCompliance.com, 800-704-3394
Bill Larson, Profit Protection Risk Management Consulting, profitprotectionmanagement@gmail.com, 801-341-2044
Judi Newman, Phaze II Consulting, Inc., judinewman@aol.com, 239-481-6001
Bob Chaput of Clearwater Compliance has recorded an excellent webinar, "What Business Associates Need to Know about HIPAA," which includes the impact of the new Omnibus Rule.
Additional written resources for Business Associates include:
Clearwater Compliance, "Preparing for the HIPAA Security Rule Again; now, with Teeth from the HITECH Act!"
ID Experts, "HIPAA Final Omnibus Playbook: Business Associate Edition"

In addition, ACT has created a prototype Agency Information Security Plan to provide a starting point for agencies. Note that agencies will need to add HIPAA specific requirements to this plan, as well as their policy for managing and securing mobile devices. For more information on managing mobile device risks, see ACT's article, "Bring Your Own Device" Opportunities & Risks.

ACT has also developed resources encouraging agencies to use TLS for secure email with business partners.

Necessary Action: Please circulate this Technical Advisory to all agency personnel that this change will apply to their area of responsibility.

This information was produced by ACT's HIPAA Work Group. ACT (Agents Council for Technology) is a part of the Independent Insurance Agents & Brokers of America, Inc. Please contact Jeff Yates, ACT's Executive Director at jeff.yates@iiaba.net with questions and comments. ACT's website is www.iiaba.net/act. This article reflects the views of the author and should not be construed as an official statement by ACT.