WHO ANSWERS YOUR PHONE? HOW YOUR ANSWERING SERVICE CAN GET YOU FINED BY HIPAA.

This series of HIPAA practice updates reflect HIPAA changes after the implementation of the Omnibus Final Rule which was published January 25, 2013 (Federal Register) with a compliance date of September 23, 2013. The HIPAA regulation changes and additions cover numerous areas of protected health information privacy and security. The failure to comply with these regulations may be associated with civil and criminal penalties and implementation must be given high priority by all healthcare providers.

Brief: The Answering Service Relationship

On February 20, 2014 at 8:00 PM an Internal Medicine specialist received a text message on his I Phone from his answering service. The message advised the physician of a patient call and described the patient’s symptoms and chief complaint. The message further provided the patient name and contact number. The event was not unusual and involved a particular relationship with the answering service involving privacy and security of information not always considered. The physician was a “covered entity (CE)” under HIPAA regulations and the answering service had been contracted for communications. Does this common situation present a potential liability?

The HIPAA Omnibus Final Rule (OFR) published in 2013 with compliance required by September 23, 2013 is very clear that liability, differing from past requirements, “...extends down the chain well beyond covered entities to reach business associates, which include certain subcontractors.” 1

The Omnibus Final Rule (OFR) among many other things changed certain definitions one of which was the definition of a “Business Associate” in §160.103 Definitions:

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 16 4.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. 2

Also the following (see note iii):

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. 3
The definition of Business Associate places answering services in the position of Business Associates. One professional organization provides the following correct guidance in partial summary of contents of the Omnibus Final Rule (OFR):

Is an answering service a BA?

“Yes, the answering service is granted access to PHI when patients disclose medical concerns that prompt them to call.” 4

In the HITECH Act signed February 17, 2009 and effective September 23, 2010 “…liability was created under the HIPAA Privacy and Security Rules for persons that are not covered entities but that create or receive protected health information in order for a covered entity to perform its health care functions, to ensure individuals’ personal health information remains sufficiently protected in the hands of these entities.” 5 Further in the Omnibus Final Rule (OFR) under “Statutory and Regulatory Background, HITECH (ii)” business associates and vendors of Personal Health Records are addressed:

“The HITECH Act is designed to promote the widespread adoption and interoperability of health information technology. Subtitle D of title XIII, entitled ‘Privacy,’ supports this goal by adopting amendments designed to strengthen the privacy and security protections for health information established by HIPAA. These provisions include extending the applicability of certain of the Privacy and Security Rules’ requirements to the business associates of covered entities; requiring that Health Information Exchange Organizations and similar organizations, as well as personal health record vendors that provide services to covered entities, shall be treated as business associates; requiring HIPAA covered entities and business associates to provide for notification of breaches of “unsecured protected health information”; establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes; prohibiting the sale of protected health information; and expanding individuals’ rights to access their protected health information, and to obtain restrictions on certain disclosures of protected health information to health plans. In addition, subtitle D adopts provisions designed to strengthen and expand HIPAA’s enforcement provisions”. 6

This corresponds to the current regulation Business Associate definition referenced earlier. 7

Knowledgeable answering services are aware of this position though the realization of being in a Business Associate position is unfortunately unknown to some covered entities and services. An example answering service website states that such services are in position of required HIPAA compliance. 8 This site correctly lists several common mistakes of answering services as:

1. “... sending unencrypted/non password protected emails containing PHI to your office or staff members”
2. “...transmitting Text Messages / SMS messages which are unencrypted/password protected....containing PHI, such as, patient name and telephone number to your office and staff members, including doctors after hours.”
3. “...sending any PHI, such as Patient Name or Telephone Number. Alpha paging transmissions are not encrypted, therefore, violate HIPAA regulations.
4. “...does not have a defined HCO (HIPAA Compliancy Officer) with the proper credentials and training,”
5. “...does not have signed Sub-Contractor Business Associate Agreements on file with all software vendors who have access to any Personal Health Information being stored or transmitted” 9

Your answering service must be HIPAA compliant including the ability to use secure methods of data transmission with avoidance of standard SMS (texting) channels. Care should be taken to have an appropriate Business Associate Agreement (BAA) in place with “satisfactory assurances” that HIPAA requirements are being followed. 10 The answering service should be able to provide positive and detailed responses to questions such as:

1. Has the service designated a HIPAA Compliance Officer (HCO)?
2. Do employees have periodic HIPAA regulation training?
3. Do messaging and Email systems incorporate security for protected health information?
4. Are periodic risk assessments made for privacy and security of health information?
5. Are Business Associate Agreements (BAA) used?

There are significant reasons to be concerned about the activities of any Business Associate. Since answering services are business associates of covered entities such as physicians a number of federal obligations under the Omnibus Final Rule (OFR) and other HIPAA regulations apply with possible civil and criminal penalties in cases of violation. These include such responsibilities as having "contracts or other arrangements with BAs to ensure that the business associates safeguard protected health information, and use and disclose the information only as permitted or required by the Privacy Rule". Also the Security Rule has required covered entities to "have contracts or other arrangements in place with their business associates that provide satisfactory assurances that the business associates will appropriately safeguard the electronic protected health information they create, receive, maintain, or transmit on behalf of the covered entities."

As stated in final HIPAA regulations “A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.”

In the earlier example situation whether or not a potential liability existed depended in large part on the proper business associate relationship being present and the security of the messaging system being used. With the Omnibus Final Rule (OFR) in 2013 adding to, changing, and finalizing earlier HIPAA regulations physicians must now take a new and careful assessment of their relationships with other businesses such as answering services.

Kenneth E. Rhea, MD, FASHRM