Answering to HIPAA

Who Answers Your Phone?

Prepared by Kenneth E. Rhea, MD, FASHRM

Brought to you by

DUXWARE™

...LEADING THE WAY IN TECHNOLOGY FOR HEALTHCARE PROVIDERS

www.duxware.com

The Event

On February 20, 2014 at 8:00 PM an Internal Medicine specialist received a text message on his iPhone 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 in practice risk analysis. 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?

Who Answers Your Phone? [1]

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."[2]

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: in 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,

"business associate definition"

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 § 164.501 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. [3]

Also the following (see in regulations section iii below):

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.** [4]

""subcontractor" is: "... a person to whom a business associate delegates a function, activity, or service"

If the medical practice utilizes an internal system for receiving calls either during normal medical working hours e.g. a member of the workforce answers call on a rotating basis section (iii) would not apply. The difference lies in the fact that the definition of a "subcontractor" is: "⋯ a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate."[5] A workforce member or employee of the medical practice is therefore not considered a subcontractor. However, while the term "answering service" is not directly addressed in either federal regulations or specifically the Omnibus Final Rule the definition of Business Associate places answering services as separate entities in the position of Business Associates.6 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." [7]

"liability was created under the HIPAA Privacy and Security Rules for persons that are not covered entities "

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."[8] Further in the Omnibus Final Rule (OFR) under "Statutory and Regulatory Background, HITECH (ii)" business associates and vendors of Personal Health Records are addressed: This information corresponds to the current regulation Business Associate definition referenced earlier.[10]

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.[11] This site correctly lists several common mistakes of answering services as:

1. Sending unencrypted/non password protected emails containing PHI to offices or staff members,

2. Transmitting Text Messages / SMS messages

"Your answering service must be HIPAA compliant including the ability to use secure methods of data transmission"

which are unencrypted/password protected…. containing PHI, such as, patient name and telephone number to offices and staff members, including to doctors after hours,

3. Sending any PHI, such as patient name or telephone number in standard SMS,

4. No 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 [12]

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.13 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) being used?

"There are significant reasons to be concerned about the activities of any Business Associate."

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".[14] 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."[15]

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

"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"

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." [16] Also a covered entity (CE) using electronic health record (EHR) systems and attempting to achieve meaningful use (MU) "… must meaningfully use certified EHR technology for an EHR reporting period, and then attest to CMS that he or she has met meaningful use for that period." [17] Meaningful Use (MU) requires under certain government objectives assuring the privacy and security of protected health information (PHI) which will include information being transmitted from business associates such as answering services. In such situations failing to assure proper privacy and security of protected health information (PHI) yet attesting to appropriate meaningful use would constitute a significant regulation violation. HHS has oversight of the federal incentive program for use of electronic health record (HER) systems and meaningful use (MU) and has undertaken audits of eligible professionals (EP) attesting to meaningful use. In fact prior HITECH regulations "…requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules." [18]

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 and that includes the use of answering services.

Questions and Answers after the Endnotes section.

(Endnotes)

[1] This article reflects 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.

[2] Pasquale F. & Ragone T.A. The Future of HIPAA in the Cloud. Seton Hall Law. Site: www.papers.ssm.com. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298158. Pub June 30, 2013. Accessed June 6, 2014

[3]US Dept Health & Human Services Office of Civil Rights. HIPAA Adminsitrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013 p 11

[4]US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013 p 11

[5]Ibid p 16

[6]US Dept Health & Human Services Office of Civil Rights. HIPAA Adminsitrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013

[7]American Osteopathic Association. HIPAA Frequently Asked Questions. Site: www.osteopathic.org http://www.osteopathic.org/inside-aoa/development/practice-mgt/hipaa/Pages/hipaa-faq.aspx. Accessed April 9, 2014

[8]Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5573

[9]Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5568

[10]US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013

[11]Patient Calls. Does a Medical Answering Service Have to be HIPAA Compliant? Site: www.patientcalls.com. http://www.patientcalls.com/answering_service_hipaa_violations.htm Accessed April 19, 2014

[12]Ibid

[13]Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5567

[14]Federal Register. Omnibus Final Rule. Government Printing Office.gov. Executive Summary and Background. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p5567

[15]Ibid

[16]US Dept Health & Human Services Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. March 26, 2013. Accessed November 4, 2013 p. §160.402 (c)(2)

[17]CMS. Guide to Privacy & Security of Health Information. Site: www.healthit.gov. www.healthit.gov/sites/default/files/privacy-and-security-guide.pdf. Accessed March 3, 2015.

[18]HHS. HIPAA Privacy, Security, & Breach Notification Program. Site. www.HHS.gov. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. Pub. April 6, 2015. Accessed April 6, 2015

Review Questions

Question 1 A physician receives in February 2015 an electronic text message (SMS standard channel) from his answering service containing information to call a patient with included the patient's name, complaints, current medications, and phone number. A correct scenario or response would be the following:

1. Based on the degree of urgency contact the patient, attempt to identify the patient and discuss the medical problem after which assurance should be obtained that the call record is being maintained by the answering service.

2. The patient medical problem should be addressed, but the message should never have been received since standard SMS is not secure or compliant with HIPAA privacy and security requirements and should not have been sent by the answering service.

3. No actions are necessary other than addressing the medical call since the answering service was contracted to provide services prior to the compliance date for the Omnibus Final Rule which extended liability to the answering service.

4. The patient call and medical problem should be addressed with continued use of SMS messaging since it has been a determination by the practice that the fastest type of communication should always be used to enhance patient safety.

Answer: 2

The practice should have had a Business Associate Agreement (BAA) in place with the answering service which would not have allowed unsecured messaging and which would have provided necessary assurances to the covered entity (CE) that necessary privacy and security was being maintained for protected health information (PHI) being held by the answering service.

Question 2 A medical practice administrator has decided after consultation with the practice physician owners to retain an answering service for limited night call weekend messages. In developing the agreement with the answering service an appropriate assurance would be to:

1. Have written assurance that all messaging to physicians by the answering service would be provided in high speed standard channel SMS for all calls,

2. Have assurance that all answering service employees have had documented HIPAA training in privacy and security regulations,

3. No calls received by the answering service would be transferred to data media storage unless directed by the employer practice Privacy Officer,

4. Any patient information held by the answering service for the medical practice would be retained in both paper and electronic form for the HIPAA required period of 2 years or longer.

Answer: 2
The answering service has the same privacy and

Kenneth E. Rhea, MD, FASHM

Dr. Rhea is a medical liability and risk consultant to medical practices and other health related organizations. He was in medical and surgical practice for over 30 years and for the past 17 years has been a consultant in medical risk and liability management. He is the owner and Managing Partner of Medical Education and Risk Consulting, called MER Consulting. Dr. Rhea has been dealing with risk and federal regulatory compliance areas such as the HIPAA privacy and security regulations beginning with the Privacy Rule in 2000.

Dr. Rhea writes monthly white papers on various sections of the HIPAA regulations in regard to those most encountered in office practice. The information will be summarized from actual federal law with both references and multiple choice questions for your teaching use.

HIPAA training is required by the regulations must be ongoing and this monthly information can be used as part of efforts to meet those requirements. These HIPAA articles can be used and documented as part of your staff and administrative training program.

While these educational materials will not by any means cover everything you need to do for HIPAA privacy and security compliance they provide more documented evidence of training and intent to comply.

If you have any questions on the information Dr. Rhea can be contacted directly. krheamd@mdriskconsulting.com

security obligations under the HIPAA regulations as the covered entity (CE) practice physicians which includes satisfactory training of the workforce in privacy and security regulations. No data should ever be transmitted to the practice physicians other than by secured transmission no matter what format,e.g. messaging, Email, etc.