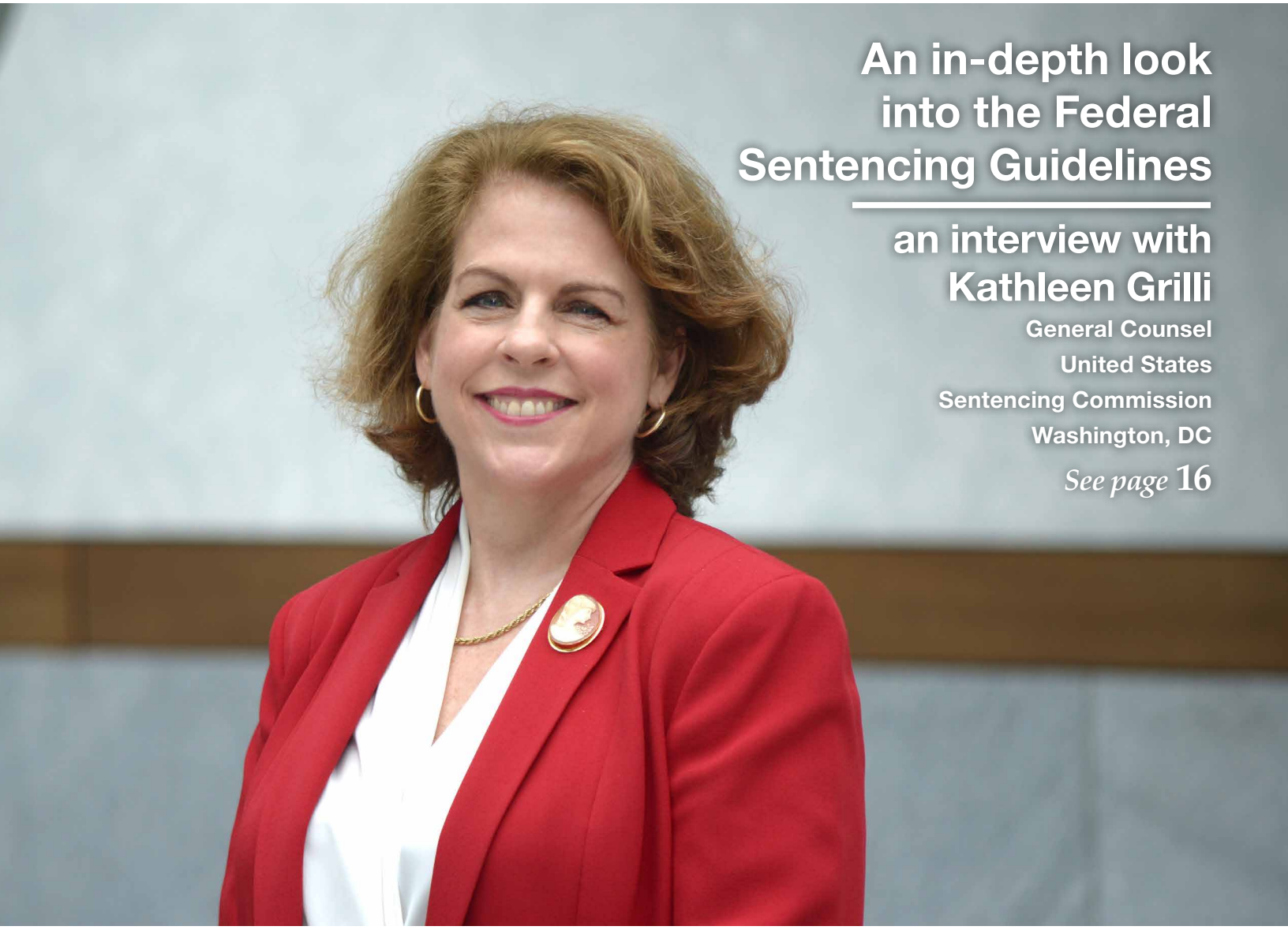
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

September 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



An in-depth look into the Federal Sentencing Guidelines

an interview with Kathleen Grilli

General Counsel
United States Sentencing Commission
Washington, DC

See page 16

24
IRO claims reviews revisited
Cornelia M. Dorfschmid

31
Guidelines for self-disclosure: Who, what, how, and when?
Gabriel Imperato

40
Ten key facts regarding the CMS overpayment rule
Joette Derricks

46
Creating and maintaining a collegial, harassment-free workplace
Scott M. Gilbert and Michael J. Lorden

by Tomi K. Hagan, Walter E. Johnson, and Frank Ruelas

HIPAA rules for unencrypted email and text messages to patients

» Text or email communications may or may not fall under HIPAA provisions.
» Consider the Privacy Rule and Security Rule when communicating to patients by text or email.
» Patients have requirements to fulfill and options to consider when requesting to receive text or email communications.
» Covered entities have an option to send encrypted or unencrypted communications to patients.
» Common pitfalls exist for covered entities that communicate to patients by text or email.

Tomi K. Hagan *(thagan@QHR.com) is a Senior Consultant of Compliance at Quorum Health Resources in Brentwood, TN.* ***Walter E. Johnson*** *(wjohnson@kforcegov.com) is the Director of Compliance and Ethics at Kforce Government Solutions, Inc. in Fairfax, VA.* ***Frank Ruelas*** *(francisco.ruelas@dignityhealth.org) is a Facility Compliance Professional with Dignity Health in Phoenix, AZ.*

/in/TomiHagan @TomiHagan
/in/Walter16 @Walter_Johnson1
bit.ly/in-FrankRuelas @Frank_Ruelas

At the 2017 HCCA Compliance Institute, representatives of the Office for Civil Rights (OCR) addressed an individual's right to access his/her protected health information (PHI) and focused attention on a very important topic that compliance professionals would do well to become familiar with that includes the use of texting and emailing to patients. Specifically, this article focuses on the sending of unencrypted emails and text messages to individuals. As we explore the do's and don'ts of the practice of texting and emailing in an unencrypted manner, we must first distinguish very clearly the nature of the message involved and its relevancy to the HIPAA Privacy and Security rules.

Does the communication include PHI?

This may sound like a very basic and simple question, but one that, with a little thought, gives us cause to pause as we look into the use of email and texting and how these may or may not be related to the Health Insurance Portability and Accountability Act (HIPAA) regulations. For example, if the unencrypted emails and texted messages do not contain PHI, then this essentially negates the HIPAA requirements, because if there is no PHI, then HIPAA would not apply.

This may sound somewhat easy and straightforward, but it may be a bit more involved when one considers how a message sent from a covered entity to an individual might be somewhat meaningless without any PHI involved. In addition to HIPAA, it is noteworthy to mention that the covered entity may have policies and procedures associated with the use of email and texting to individuals that the compliance professional (HIPAA


Hagan


Johnson


Ruelas

issues aside) would do well to identify and become familiar with in their implementation.

So now that we have looked at the use of unencrypted email and texting for communications that do not contain PHI sent between a covered entity and an individual, let's look into the use of these communication options and how they may relate to compliance efforts with respect to the HIPAA Privacy and Security Rules when PHI is involved.

HIPAA Privacy and Security

The use of unencrypted texts and emails containing PHI is going to fall under the scope of both the HIPAA Privacy Rule and the Security Rule. The Privacy Rule applies because it involves PHI in all of its forms, and we have the issue of an individual's right to access his/her PHI to consider. However, the use of unencrypted texts and emails that may contain PHI is going to also fall squarely within the scope of the Security Rule, because the Security Rule specifically deals with PHI that is in an electronic format.[1] Therefore, we need to understand how the Security Rule addresses the sending of unencrypted PHI.

Let's first look at the question of sending PHI in an unencrypted manner. We are fortunate here because with respect to encryption, the Security Rule provides some clear direction on the application of encryption.

Unencrypted PHI under the Security Rule

Under the Security Rule, there is an addressable implementation specification that relates to encryption. We need to remember that when we see an addressable implementation specification in the Security Rule, we have two clear paths that we may take.[2]

The first path is for us to implement the specification as presented. So if we opted for this path, we would adopt the use of encryption and apply it. When one considers the many benefits of encryption to both the sender and the receiver, as well as the ways encryption may help avoid a breach, it is very easy to see why many organizations opt to adopt encryption. When sending encrypted email, remember that the encryption may only apply to the body of the email and attachments. Use caution when placing a title on the email subject line, because PHI in the subject line will likely not be encrypted. The benefits of using encryption can be negated by inattention to the subject line.

The second path is also relatively straightforward with a slight twist on the first. We have the option of documenting why we believe the implementation of the standard (encryption in this case) is not reasonable, and then we must do something that is often overlooked. We must then apply what is often referred to as an Alternative Equivalent Measure (AEM). So essentially, we have the option of encryption or the use of an AEM that basically provides the same type of safeguard that encryption presents. Given the very unique and specific safeguards provided by encryption, one would be hard-pressed to identify, much less apply, an AEM to encryption.

So under the Security Rule, it appears that sending unencrypted texts or emails is not an option. However, this does not shut the door on the texting or emailing of unencrypted communications that may contain PHI to individuals. As we were reminded by the OCR, the window of opportunity to send unencrypted emails or texts is wide open and is presented to us by the Privacy Rule.

Unencrypted PHI and the Privacy Rule

To understand the use of unencrypted texts and emails containing PHI, we need to understand when doing so would be appropriate under the Privacy Rule. To do that, we must revisit the topic of an individual's right to access to PHI.

One of the main rights afforded individuals under the HIPAA rules is the right of the individual to access his/her PHI.[3] Most compliance professionals are familiar with this right, which has existed since the original rules were implemented. However, in 2013 with the release of the Omnibus Rule, there was the introduction of an additional requirement that may be imposed on the covered entity by the individual if the individual directs the covered entity to transmit ePHI electronically to another party identified by the individual.

Requirements and options

In order for an individual to require the covered entity to transmit PHI (which could include by means of an email or text), there are some requirements that must be met. First, the request must be in writing. Second, the individual must clearly identify where the PHI is to be sent. For example, if the PHI is to be sent by email, the email of the recipient needs to be provided to the covered entity. If the PHI is to be sent by text, the text address (which may either be an email address or a mobile device's phone number) needs to be provided to the covered entity. Third, the covered entity has a duty to inform the individual making the request that the PHI sent by an unencrypted method may be accessed by unauthorized recipients and that the individual acknowledges and accepts the risk.[4]

Once these requirements are met, then the covered entity may proceed with sending an unencrypted email or text that contains the identified PHI. Does this mean that the covered entity must always send PHI directed to a third party in an unencrypted manner? Not at all. We are simply pointing out that if an individual requests PHI to be sent in an unencrypted manner, there is a process for doing this that is described in the HIPAA regulations. In fact, exploring the option of sending the PHI in an encrypted manner rather than unencrypted may actually be preferred by all involved.

Choosing encryption over no encryption

Some covered entities use encrypted texting and email technologies that allow for the sending of PHI. These can be used to send PHI in a manner that both safeguards the privacy and security of the PHI, but also provides a means for the covered entity to avoid a possible breach if the encrypted text or email finds its way to an unintended recipient, provided that the encryption makes the PHI unusable, unreadable, and indecipherable.[5]

It is not unusual for an individual who makes a request for an unencrypted text or email to reconsider his/her request and opt for the use of encryption after someone from the covered entity has explained the benefits of protecting the privacy and security of the individual's PHI. Often, individuals request unencrypted email to avoid the extra steps involved in retrieving encrypted transmissions or out of fear that they will not be able to access the information. Explaining the process and providing clear instructions for retrieval may resolve these concerns. Some individuals may still decline the use of an encryption-based solution; however, offering the individual an option may also motivate the individual to select a more secure option rather than one that is unencrypted.

To further one's commitment in trying to safeguard the security and privacy of an individual's PHI, consider the following when meeting the documentation requirements as previously described. Include a notation on whatever documentation was used to meet the HIPAA requirements that the individual was provided information on the availability of a secure texting or email option, which the individual declined to use.

Avoiding pitfalls to unencrypted communication

Remember that patients may not possess the same level of technical savvy as the compliance or privacy professional. Take steps to ensure that patients actually understand the risks of unencrypted email, including the possibility of a breach, and are able to make an informed decision. If a breach were to happen, a patient could claim that they were not adequately warned of the risks of unencrypted communication.

The requirements for the covered entity transmittal of PHI do not vary based on who initiated the communication. An unencrypted email or text from a patient should not be treated as permission for the covered entity to respond in the same manner. The documentation requirements still apply, and the patient must be informed of the risks prior to the covered entity's response.

Errors in email addresses or phone numbers may lead to impermissible disclosures. Consequently, impermissible disclosures are presumed to be breaches as defined in the HIPAA regulations and could trigger the required breach notification requirements.[6] Whether the incorrect information was provided by the patient or the covered entity made the error, investigation and any notifications from the resulting breach will still be the responsibility of the covered entity.[7] Taking measures to verify email addresses and phone numbers prior to transmitting PHI is an effective risk-mitigation strategy to reduce the likelihood that PHI will be sent incorrectly to an unintended recipient.

Conclusion

Meeting the HIPAA privacy and security requirements to both provide individuals' access to their PHI and to protect that PHI can be challenging for compliance and privacy professionals. Clear communication to patients may limit the use of unencrypted communication. When patients do choose to receive unencrypted emails or texts, consistent application of the rules and documentation can reduce risk to the organization.

Walter E. Johnson contributed to this article in his personal capacity. The views expressed are his own and do not necessarily represent the views of Kforce Government Solutions, Inc.

1. http://bit.ly/2xfGtBD, pg 4.
2. 45 CFR §164.306(d)(1)
3. 45 CFR §164.524(a)(1)
4. Federal Register, January 25, 2013 (Volume 78, Number 17)
5. Federal Register, April 27, 2009 (Volume 74, Number 79)
6. 45 CFR §164.402
7. 45 CFR §164.414(b)

Correction – August 2017 Compliance Today, "HIPAA compliance: Is your dental organization ready?"

The information on page 74, Grid: Breach Notification Rule: 45CFR 164,400-414, is incorrect. The following is correct.

Accordingly, in the Final Rule, HHS revised the definition of a "breach" to state that unless an exception applies, an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Further, to determine whether there is a low probability that the PHI has been compromised and whether breach notification is necessary, the covered entity or business associate, as applicable, must conduct a risk assessment that considers, at a minimum, each of the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.