HITECH Frequently Asked Privacy, Security Questions

By Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA

Editor's note: This is the first installment of a three-part series reviewing AHIMA's HITECH Frequently Asked Questions.

This month marks the one-year anniversary of the publication of the final HITECH Omnibus Rule, which became effective March 26, 2013. Covered entities and business associates (BAs) were expected to meet compliance by September 23, 2013.

The Omnibus Rule expanded some of HIPAA's original requirements involving the privacy, security, and enforcement components. It also finalized the Breach Interim Final Rule as well as the Genetic Information Nondiscrimination Act (GINA). Organizations have been busy since the January 2013 publication date updating policies and procedures, educating and training staff, and—more importantly—ensuring that the interpretation and understanding of the new rules is applied appropriately.

AHIMA has created a list of the most frequently asked questions regarding the HITECH Omnibus Rule. This section will share those questions and answers in a three-part series to provide guidance and clarify some confusion about the rule. Part I of this series will highlight the updated requirements for a patient's right to electronic access of their protected health information (PHI), as well as the requirements for the Notice of Privacy Practices (NPP).

Notice of Privacy Practices FAQ

The Notice of Privacy Practices for Protected Health Information (NPP) section of the HITECH Act—Section 164.520—defined new requirements for the NPP, including redistribution.[1] HITECH also included the following provisions:

- The final rule modifies §164.520(b)(1)(ii)(E) requiring certain statements on the NPP about uses and disclosures that require authorization.
- Redistribution requirements were updated for health plans, but remained the same for providers.

Q: What exactly is the rule for redistributing the NPP after significant changes have been made to it? Would the Omnibus Rule changes be considered significant?

A: Yes, the rule features significant changes that require patient notification. For healthcare providers with direct treatment relationships, this means that, by the September 23, 2013 compliance date, they should have revised the notice that is posted in waiting areas, on their website, that is provided to new patients, and is available upon request to existing patients.

Q: Does the NPP have to include a statement if the covered entity plans on sending out appointment reminders?

A: The new rule removes this requirement. Covered entities are free to leave this in or remove it from the notices.

Q: Once changes are made to the NPP, do patients need to re-sign it?

A: No. For healthcare providers, the final rule does not modify the current requirements to distribute revisions to the NPP. As such, if a healthcare provider with a direct treatment relationship with an individual revises the NPP, the healthcare provider must make the NPP available upon request on or after the effective date of the revision and must have the NPP available at the care delivery site. They must also post the notice in a clear and prominent location.

The Office for Civil Rights (OCR) clarifies that providers are not required to print and hand out a revised NPP to all individuals seeking treatment. Instead providers must post the revised NPP in a clear and prominent location and have copies

of the NPP at the care delivery site for individuals to request and take with them. Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment receipt from, new patients.

Q: What statement(s) must be added to the new NPP?

A: Refer to AHIMA's NPP Practice Brief [...], or to the US Department of Health and Human Services OCR Model NPPs, available online at www.healthit.gov/providers-professionals/model-notices-privacy-practices.

Electronic Access FAQ

Section 164.524 of the HITECH Act covers the "access of individuals to protected health information." Covered entities must provide an electronic copy of protected health information that is maintained electronically, located in one or more designated record sets, and is in the form and format requested.

This section also expressly requires that when an individual requests the covered entity to transmit a copy of the protected health information (PHI) to another person, the covered entity must comply. Within this provision, the request must:[2]

- Be made in writing
- Be signed by the individual
- Clearly identify the designated person
- Clearly identity where the information will be sent

Finally, this section discusses labor costs and what can and cannot be included in a reasonable cost-based fee for providing copies.

Q: What can be included as part of billable labor costs when determining fees for record requests?

A: This provision allows for identifying the labor for copying protected health information, whether in paper or electronic form. Labor costs can include a reasonable cost-based fee for skilled technical staff time spent creating and copying electronic files and doing work like compiling, extracting, scanning, burning onto media, or distributing media. This could also include the time spent preparing an explanation or summary.

Other fees include a cost of supplies for creating the paper copy or electronic media (if the individual requests portable media), and postage or courier costs.

This provision clarifies that a covered entity may not charge for a retrieval fee, whether it is a standard retrieval fee or one based on actual retrieval costs.

Q: The cost of copying health information is set by state law, which is used by the copy service. How do we determine cost per page taking into account state law?

A: The Omnibus Rule preamble explicitly states that covered entities need to determine if the fee is reasonable. When a state law provides a limit on the fee that a covered entity may charge for a copy of protected health information, this is relevant in determining whether a covered entity's fee is ''reasonable.''

A covered entity's fee must be both "reasonable" and "cost-based." For example, if a state permits a charge of 25 cents per printed page, but a covered entity is able to provide an electronic copy at a cost of 5 cents per page, then the covered entity may not charge more than 5 cents per page—since that is the reasonable and cost-based amount.

Similarly, if a covered entity's cost is 30 cents per page but the state law limits the covered entity's charge to 25 cents per page, then the covered entity may not charge more than 25 cents per page. This is because charging 30 cents per page would be the cost-based amount, but would not be reasonable in light of the state law.

Q: Does a covered entity or business associate have to release existing paper records in electronic media, if requested? Would the charge then be by page count or electronic media?

A: An entity has to provide the copy in the form and format requested, if readily producible. There is a lack of clarity, though, on what is meant by "readily producible." The preamble does indicate that you are not required to scan paper documents to provide electronic copies. Accordingly, providing paper copies remains permissible. While there is nothing in the law that precludes facilities from agreeing to scan the documents and convert them into electronic media, it may be best to inform individuals of the potential costs of scanning and converting records to electronic media before doing so.

Q: Can a covered entity send PHI via unencrypted e-mail? For example, a patient requests that their PHI be sent to their Yahoo or Gmail e-mail account. Is this permitted?

A: The following is HHS' clarification on this topic: "We [HHS] clarify that covered entities are permitted to send individuals unencrypted e-mails if they have advised the individual of the risk, and the individual still prefers the unencrypted e-mail. We do not expect covered entities to educate individuals about encryption technology and information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the e-mail could be read by a third party.

If individuals are notified of the risks and still prefer unencrypted e-mail, the individual has the right to receive protected health information in that manner, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual."

Notes

1. AHIMA. "Analysis of Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rule." January 25, 2013.
2. Ibid.

Angela Dinh Rose (angela.rose@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Rose, Angela Dinh. "HITECH Frequently Asked Privacy, Security Questions" *Journal of AHIMA* 85, no.1 (January 2014): 50-51.