PRIVACY ALERT
July 31, 2017

Individual's "Right" to Unencrypted E-Mails Limited

OCR's FAQ Applies only to Individual's Request to Access his/her PHI

The Department of Health and Human Services' Office for Civil Rights (OCR) recently published a "Frequently-Asked Question" indicating that an individual has a right to receive copies of protected health information "by unsecure methods if that is her preference." At least one large business associate has interpreted this to mean that it may use unsecure e-mails and texts to send detailed protected health information to an individual who elects to receive information in that manner, notwithstanding contractual provisions that require the business associate to use only abbreviated protected health information in such communications. A health plan that adopts this position for sending members routine communications—or that permits its business associate to do so—may violate the HIPAA Privacy and Security Rules.

The OCR FAQ, which is available here, explains that:

> "individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual's PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail. If the individual says yes, the covered entity ***must comply with the request***." (Emphasis added.)

But, the FAQ does not apply to ***all*** communications a covered entity makes to an individual. In fact, the FAQ is limited to a single type of communication: a covered entity's response to an individual's request to exercise his/her right to "access" his/her protected health information.

The Privacy Rule grants individuals the right to access protected health information that a covered entity maintains in a "designated record set." The HITECH Act expanded this right by requiring (among other things) that a covered entity provide the information in an electronic format upon request. And the Department of Health and Human Services further expanded this right in the HIPAA Rules Omnibus Amendments (published in 2013),

by requiring covered entities to honor an individual's request for access by making the individual's protected health information available "in the form and format requested by the individual."

The OCR FAQ explains how this right applies when an individual who has exercised his/her right to access protected health information prefers to receive the information in an unsecure manner. Once the covered entity explains the risks of sending the individual protected health information in an unsecure manner, the individual has the right to accept the risk and receive the information "in the form and format requested." But the individual's right to dictate the form and format of communications containing protected health information applies ***only*** to a covered entity's response to the individual's request for access—not to a covered entity's routine communications with the individual. This is why the FAQ was originally published on the OCR webpage, entitled "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." (Click here and search for the phrase "the right under HIPAA").

A health plan's routine communications with its members remain subject to the Privacy Rule's minimum necessary limitation. Moreover, the Security Rule requires a health plan that elects (or permits its business associate to elect) not to encrypt e-mails or texts that contain protected health information to document the decision. Specifically, a health plan must document why using unsecure e-mails or texts is reasonable and appropriate under the circumstances, after having considered the following four factors:

- The size, complexity, and capabilities of the health plan.
- The health plan's technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to electronic protected health information.

Thus, a health plan should not decide (and should not permit its business associate to decide) to use unencrypted e-mails or texts to send members detailed protected health information in routine communications based on this OCR FAQ.

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or
TBixby@tbixbylaw.com

Thomas D. Bixby Law Office LLC
(608) 661-4310 | www.tbixbylaw.com