Patient rights to protected health information under HIPAA

Most people with even a basic knowledge of the HIPAA regulations understand that HIPAA permits covered entities to disclose protected (identifiable) health information (PHI) for “treatment, payment and health care operations” without the need to first obtain authorization from the patient. For some other uses or disclosures, such as marketing and research, the patient’s prior authorization is required (although the authorization requirement for research can be waived). Other provisions provide that information can be shared – such as with family members or in general facility directories – unless the patient has clearly objected.

What is often not emphasized in these provisions is that the HIPAA privacy rule “permits” the sharing of health information under these circumstances, but does not require it. For example, a provider caring for a patient is allowed to share data with other treating providers for treatment purposes – but HIPAA does not mandate that this sharing occur.

In contrast, HIPAA requires the sharing of health information in two specific instances: with the patient when the patient requests access to or a copy of his or her PHI, and with the government when the covered entity is being investigated for possible violations of HIPAA. Consequently, patients have greater rights with respect to the sharing of their health information than other health care providers.

The specific provision providing patients with the right to access or obtain a copy of his or her PHI allows patients to receive this information “in the form or format requested by the individual, if it is readily producible in such form or format…”

HITECH clarified that patients have the right to obtain copies of their health data in electronic form (and have those copies digitally transmitted directly to a third party) if the data they are requesting is maintained electronically. In the recent regulations finalizing those provisions (referred to as the Omnibus), the HHS Office for Civil Rights, which has oversight over HIPAA, clarified how entities are to manage patient requests for digital data in particular formats.

Many covered entities have presumed that protected health information sent to patients would need to be sent securely consistent with the HIPAA Security Rule. But the Omnibus clarified this as well, making clear that if the patient requests his or her protected health information in an unencrypted form – such as by unencrypted e-mail – the patient has the right to receive it in this form. Covered entities have an obligation to be certain the patient knows that receiving the protected health information in this form is not secure and to confirm that the patient still wants it in this format – but once that is done (and a burdensome, detailed warning is not expected), the patient has the right to his information “in the form or format requested,” even if the form requested is not secure.

Here, excerpted directly from the Omnibus rule, is the precise language on this point:

Comment: Several commenters specifically commented on the option to provide electronic protected health information via unencrypted email. Covered entities requested clarification that they are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. Some felt that the ‘‘duty to warn’’ individuals of risks associated with unencrypted email would be unduly burdensome on covered entities. Covered entities also requested clarification that they would not be responsible for breach notification in the event that unauthorized access of protected health information occurred as a result of sending an unencrypted email based on an individual’s request. Finally, one commenter emphasized the importance that individuals are allowed to decide if they want to receive unencrypted emails.

Response: We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the ‘‘duty to warn’’ individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the 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 email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, 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.[[1]](#footnote--1)

This guidance was provided in the context of implementing an individual’s right under HITECH and HIPAA to get electronic access to their protected health information, but there is no reason why different standards would apply with respect to any communications between a health care provider and patient. If the patient wants those communications via a methodology that is more convenient for them – but is unsecure – the provider should be able to meet the patient’s wishes, without being in violation of the HIPAA Security Rule, as long as the safeguards above re: transparency to the patient and confirming the patient’s wishes, are honored.

1. 78 Fed. Reg. 5634 (January 25, 2013). [↑](#footnote-ref--1)