CLIENT ALERT

Key Takeaways from HIPAA Guidance on Individuals' Rights to Access Health Information

Jan.21.2016

On January 7, 2016, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued guidance on an individual's right to access health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR § 164.524). This guidance reflects the Administration's focus on promotion of patient access to data and patient-driven care.

This guidance does not establish new requirements. It clarifies areas of confusion related to individuals' rights and covered entities' requirements to improve institutional compliance, particularly in light of the proliferation of electronic health records and electronic health information. OCR highlighted areas where it believes covered entities historically have failed to comply with the HIPAA access requirements, which may indicate OCR intends to step up enforcement in these areas. Here are some key takeaways from the guidance:

- Covered entities should be able to readily produce electronic information in electronic form and provide protected health information (PHI) via mail and email.
- Many barriers to access are contrary to the Privacy Rule, such as requiring a physical visit or use of a web portal to make requests, charging inappropriate fees, or requiring that individuals provide a reason for their request.
- The HIPAA access right differs from the CMS Electronic Health Records (EHR) Incentive program patient access requirements. Compliance with both is required.

General Right to Access

The Privacy Rule generally requires HIPAA covered entities to provide individuals with access to their PHI in one or more "designated record sets" (45 CFR § 164.501) maintained by or for the covered entity. Designated record sets extend beyond information maintained in an electronic health record or patient medical record, and they include any individually identifiable information used to make decisions about individuals, such as billing records, medical images, wellness and disease management program files, and clinical case notes.

Requests for Access

Method of Access

The Privacy Rule requires that entities provide access to PHI in the form and format requested. If that option is not readily producible, the PHI must be provided in a readable hard copy form or other form agreed to by the entity and the requestor. If the request for an electronic copy relates to a document maintained electronically, the entity must produce it electronically. It must be in the electronic form and format requested by the individual if it is readily producible in that form and format (even if the covered entity would prefer to provide access in a different electronic form and format).

Covered entities must also meet manner of access requirements, including arranging a convenient time and location for an individual to pick up the PHI or sending the PHI by mail or email at the request of the individual. Covered entities are not responsible for a disclosure of PHI while in transmission to the individual. The guidance also references the new requirement for certified EHR technology to enable application programming interface (API) functionality to allow patients to use the application of their choice to access their data. The guidance does not, however, assert that use of APIs is required under HIPAA.

Requirements for Requesting Access

The Privacy Rule requires covered entities to take reasonable steps to verify the identity of the individual making a request, though the method of verification is at the entity's discretion. Verification may not create barriers or unreasonably delay an individual's access to PHI. Unreasonable measures include requiring a person to physically come into the office, use a web portal, or use paper mail to make such a request, and entities are encouraged to offer multiple means to make requests.

Fees

Covered entities may impose a cost-based fee for the PHI request. Fees may only include the cost of labor for copying the PHI, supplies for creating the copy, postage, as applicable, and preparation of a summary of the PHI, as applicable. The fee cannot include any other costs, even if other costs are authorized by State law. Impermissible costs include costs of verification, documentation, searching for and retrieving the PHI, maintaining systems, and recouping capital for data access, storage, or infrastructure.

Denial of Access

In its guidance, OCR clarifies that under **very** limited circumstances, a covered entity may deny an individual's request for access to all or a portion of the PHI requested. A covered entity may **not** require an individual to provide a reason for requested access. The individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access. Further, an entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the requested PHI .

Relationship Between HIPAA and EHR Incentive Program Access Requirements

Under the CMS EHR Incentive Program, eligible providers may receive incentive payments and avoid payment reductions by demonstrating meaningful use of Certified EHR Technology. The EHR Incentive Program requires participating providers to give patients the ability to access their health information and ensure that patients can actually access that data or transmit it to a third party.

The requirements overlap with HIPAA but differ in important respects. Specifically, the EHR Incentive Program applies to a smaller set of health information, a "common clinical data set" (45 CFR § 170.102), while the HIPAA Privacy Rule applies to all information in a "designated record set," a much broader set of data. In addition, the EHR Incentive Program requires health information to be available within days, whereas the HIPAA Privacy Rule allows up to 30 days to make health information available. Ultimately, if an entity participates in the EHR Incentive Program and is covered by HIPAA, the entity must comply with **both** the EHR Incentive Program requirements and the HIPAA Privacy Rule, and the more stringent of the two requirements

when they overlap. Despite the differences, it is possible for a provider to leverage its Certified EHR Technology to fulfill its HIPAA Privacy Rule access obligations.

Conclusion

We recommend that covered entities review their HIPAA compliance practices in light of this guidance, particularly to ensure compliance with the 2013 HIPAA modifications and to ensure their policies and practices are consistent with both the HIPAA Privacy Rules and the EHR Incentive Program requirements.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com

Roma Sharma
Counsel – Washington, D.C.
Phone: +1 202.624.2784
Email: rsharma@crowell.com