OCR Issues Clarifying Guidance on HIPAA’s Individual Access Right

On January 7, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) issued guidance on the Health Insurance Portability and Accountability Act’s (HIPAA) right of individuals to access and obtain a copy of their protected health information (PHI).

While the HIPAA Privacy Rule has always provided individuals with the right to access and receive a copy of their PHI held by healthcare providers and health plans or their business associates, OCR discovered from recent studies and its own enforcement experience that individuals often face obstacles to accessing their health information — even from the covered entities required to comply with the HIPAA Privacy Rule. It is no surprise that given its focus on protecting privacy rights, OCR emphasizes the critical nature of the right of access, notes that there are limited exceptions to the right and admonishes covered entities that activities impeding access will not be tolerated. As such, the guidance potentially signals increased enforcement where covered entities do not honor requests for access as required by HIPAA.

To promote greater access to health information, OCR released a fact sheet and the first in a series of topical frequently asked questions (FAQs) that address the scope of information covered by HIPAA’s access right (e.g., clarifying what is considered a designated record set), the narrow exceptions to this right (e.g., information that would be excluded and the grounds for denial of access) and other mandated elements, including timeliness, the form and format for individual requests for access and the form and format for providing access.

Among other important issues, OCR clarifies the types of records that may or may not be considered designated record sets. Notably, OCR explains that certain records that may be generated from and include an individual’s PHI may not be considered part of the designated record set, as they are not used to make decisions about individuals. For example, quality assessment or improvement records, patient safety activity records, and business planning, development and management records that are used for business decisions more generally rather than to make decisions about individuals — such as a hospital’s peer review files, practitioner or provider performance evaluations, or a health plan’s quality control records that are used to improve customer service, or formulary development records — are typically not considered part of a designated record set.

With respect to the requirement that a covered entity provide an individual with access to PHI in the form and format requested, OCR emphasizes that covered entities must accommodate individual requests regarding the form or format of requested PHI where the covered entity has the capability to do so and contemplates
negotiations between covered entities and individuals to arrive at mutually agreeable formats. For example, where an individual requests an electronic copy of PHI that a covered entity maintains only on paper, the guidance clarifies that a covered entity is required to provide the individual with an electronic copy if it is readily producible electronically (e.g., the covered entity can readily scan the paper record into an electronic format) and the electronic format requested if readily producible in that format or, if not, in a readable alternative electronic or hard-copy format as agreed to by both the covered entity and the individual.

While OCR acknowledges that a covered entity may charge a reasonable cost-based fee for providing access to an individual’s PHI, it clarifies that the fee may not include costs associated with verification, documentation, searching for and retrieving the PHI, maintaining systems, recouping capital for data access, storage or infrastructure or other costs not listed here even if authorized by state law.

Although much of the guidance simply restates prior guidance, it includes many new facets. Among other provisions, the guidance clarifies that covered entities:

- are not required to create new information, such as explanations;
- may require the use of their own forms for requests for access, provided the form does not create a barrier or unreasonably delay the individual from obtaining access to his/her PHI;
- may not require an individual to physically come to a facility to pick up his/her records, demand payment of a bill prior to release of records or insist that an individual submit a request through a Web portal;
- may not require an individual to give a reason why he/she is requesting access; and
- are not liable if they comply with an individual’s access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit.

Lastly, OCR also covers how the HIPAA access right intersects with patient access requirements under the Electronic Health Record (EHR) Meaningful Use and Incentive Program. Specifically, the guidance addresses situations where the individual requests access to his/her PHI via the functionality of the covered entity’s certified EHR technology. For example, the guidance provides that an individual could request a copy of the information that constitutes the specific set of data known as the Common Clinical Data Set through the provider’s certified EHR technology portal or that it be sent from the certified EHR technology to the individual’s Direct address (an electronic address for securely exchanging health information using the Direct technical standard). Or, if the individual is not aware of the EHR Meaningful Use and Incentive Program, the hospital may inform the individual of these options, and, if the individual agrees to the portal access, the provider will be able to satisfy the individual’s HIPAA access request using the certified EHR technology portal.

The complete first installment of OCR’s guidance and FAQs on the individual right of access to PHI can be found here.

OCR plans to develop additional guidance and other tools as necessary to ensure that individuals understand and can exercise their right to access their PHI. In addition, OCR will be working with the White House Social and Behavioral Sciences Team and the Department of Health and Human Services Office of the National Coordinator for Health Information Technology to produce consumer-friendly resources, including sample communications tools to encourage patients to access their digital health information.
If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Anna L. Spencer
Partner
+1 202 736 8445
aspencer@sidley.com

Meenakshi Datta
Partner
+1 312 853 7169
mdatta@sidley.com

Rina Mady
Associate
+1 312 853 6109
rmady@sidley.com

Sidley Healthcare Practice
Our Healthcare Practice represents participants in all facets of the healthcare industry, including pharmaceutical, biotech and device companies, DME suppliers, hospitals, skilled nursing facilities, physician-owned companies, professional associations and research institutions. Our lawyers combine a strong background in the complexities of healthcare financing and delivery, including coding, reimbursement, and coverage issues, privacy and security, trade regulation, and competition. We have extensive experience representing clients on enforcement and regulatory matters before federal and state enforcement agencies.

For further information on the Healthcare Practice, please contact:

Paul E. Kalb, M.D.
+1 202 736 8050
pkalb@sidley.com

Richard D. Raskin
+1 312 853 2170
rraskin@sidley.com

Sidley Privacy, Data Security & Information Law Practice
We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property and criminal issues.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.